Part No. 209322-C
November 2001

4401 Great America Parkway
Santa Clara, CA 95054

Reference for the Business Policy Switch 2000 Management Software Operations Software Version 2.0

NORTEL NETWORKS™

Copyright © 2001 Nortel Networks

All rights reserved. November 2001.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks NA Inc.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license. The software license agreement is included in this document.

Trademarks

BayStack, Business Policy Switch 2000, Nortel Networks, the Nortel Networks logo, and Optivity are trademarks of Nortel Networks.

Microsoft and Windows are registered trademarks of Microsoft Corporation.

Java is a trademark of Sun Microsystems Incorporated.

Acrobat Reader and Adobe are registered trademarks of Adobe Systems, Incorporated.

All other trademarks and registered trademarks are the property of their respective owners.

Restricted rights legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks NA Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks NA Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Nortel Networks NA Inc. software license agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying software or installing the hardware unit with pre-enabled software (each of which is referred to as "Software" in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH NORTEL NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

1. License grant. Nortel Networks NA Inc. ("Nortel Networks") grants the end user of the Software ("Licensee") a personal, nonexclusive, nontransferable license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID, for which it was originally acquired; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Nortel Networks Agent software or other Nortel Networks software products. Nortel Networks Agent software or other Nortel Networks software products are licensed for use under the terms of the applicable Nortel Networks NA Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Nortel Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Nortel Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Nortel Networks' and its licensors' confidential and proprietary intellectual property. Licensee shall not sublicense, assign, or otherwise disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Nortel Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee's facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Nortel Networks warrants each item of Software, as delivered by Nortel Networks and properly installed and operated on Nortel Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Nortel Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Nortel Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Nortel Networks will replace defective media at no charge if it is returned to Nortel Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee's intended results and for the installation, use, and results obtained from the Software. Nortel Networks does not warrant a) that the functions contained in the software will meet the Licensee's requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Nortel Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Nortel Networks or in accordance with its instructions; (ii) used in conjunction with another vendor's product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED,

INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL NORTEL NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF NORTEL NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO NORTEL NETWORKS FOR THE SOFTWARE LICENSE.

5. Government licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Nortel Networks of any such intended examination of the Software and may procure support and assistance from Nortel Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Nortel Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Nortel Networks copyright; those restrictions relating to use and disclosure of Nortel Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Nortel Networks the Software, user manuals, and all copies. Nortel Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Nortel Networks, 4401 Great America Parkway, P.O. Box 58185, Santa Clara, California 95054-8185.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN NORTEL NETWORKS

AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST NORTEL NETWORKS UNLESS NORTEL NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

Preface 23

Before you begin 23
Text conventions 23
Related publications 24
How to get help 25

Chapter 1
Device Manager basics 27

Starting Device Manager 27
Setting the Device Manager properties 28
Opening a device 30
Device Manager window 33
Menu bar 34
Toolbar 35
Device view 35
Selecting objects 36
Selecting a single object 36
Selecting multiple objects 37
Viewing information about an MDA 37
Media dependent adapters and port conventions 38
LEDs and ports 39
Shortcut menus 40
Status bar 42
Using the buttons in Device Manager dialog boxes 42
Editing objects 43
Working with statistics and graphs 44
Types of statistics 44
Types of graphs 44

Statistics for single and multiple objects 47
Viewing statistics as graphs 48
Telneting to a switch 50
Trap log 51
Online Help 52

Chapter 2
Configuring and graphing the switch 53

Viewing switch IP information 53
Globals tab 53
Addresses tab 54
ARP tab 55
Editing the chassis configuration 56
System tab 57
Base Unit Info tab 60
Stack Info tab 62
Agent tab 64
SNMP tab 65
Trap Receivers tab 67
Editing network traps 67
Power Supply tab 68
Fan tab 69
CPU/Mem Utilization tab 71
Working with configuration files 72
Graphing chassis statistics 74
SNMP tab 75
IP tab 78
ICMP In tab 81
ICMP Out tab 83

Chapter 3
Configuring and graphing ports 85

Viewing and editing a single port configuration 85
Interface tab for a single port 86
VLAN tab for a single port 89

STG tab for a single port 91
EAPOL tab for a single port 93
Viewing and editing multiple port configurations 96
Interface tab for multiple ports 96
VLAN tab for multiple ports 99
EAPOL tab for multiple ports 100
Graphing port statistics 102
Interface tab for graphing ports 103
Ethernet Errors tab for graphing ports 105
Bridge tab for graphing ports 109
RMON tab for graphing ports 110
EAPOL Stats tab for graphing ports 113
EAPOL Diag tab for graphing ports 114

Chapter 4
Setting up MultiLink Trunk ports 119

MultiLink Trunk (MLT) features 119
Setting up MLTs 120
Adding ports to a MultiLink Trunk 120
MultiLink Trunk statistics 121
MultiLink Trunk Ethernet error statistics 123

Chapter 5
Creating and managing VLANs 127

VLANs 127
Creating VLANs 128
VLAN information 128
Creating a port-based VLAN 129
Creating a protocol-based VLAN 131
Creating a source address MAC-based VLAN 133
Accepting tagged and untagged frames 136
Snoop tab 137
Modifying and managing existing VLANs 138
Deleting LANs 139

Chapter 6
Creating and managing multiple STGs 141

STGs 141
Configuring STGs 142
Viewing STG configuration 143
Creating an STG 144
Adding a VLAN to an STG 146
Moving a VLAN between STGs 146
Deleting an STG configuration 146
Displaying STG status 147
Displaying STG ports 148

Chapter 7
Configuring QoS 151

Managing interface groups 151
Displaying interface queues 151
Displaying interface groups 153
Assigning ports to an interface group 154
Deleting ports from an interface group 155
Adding interface groups 155
Deleting interface groups 156
Displaying interface IDs 157
Displaying priority queue assignments 158
Displaying priority mapping 159
Displaying DSCP queue assignments 160
Displaying DSCP mappings 161
Managing QoS rules 163
Displaying IP filters 163
Adding IP filters 164
Deleting IP filters 165
Displaying IP filter groups 165
Adding IP filter groups 166
Deleting IP filter groups 167
Displaying Layer 2 filters 167
Adding Layer 2 filters 169

Deleting Layer 2 filters 170
Displaying Layer 2 filter groups 170
Adding Layer 2 filter groups 171
Deleting Layer 2 filter groups 172
Managing QoS actions, meters, shapers, and policies 173
Displaying QoS actions 173
Adding QoS actions 174
Deleting QoS actions 175
Displaying QoS meters 175
Adding QoS meters 176
Deleting QoS meters 177
Displaying QoS shapers 178
Adding QoS shapers 179
Deleting QoS shapers 180
Displaying QoS policies 181
Adding QoS policies 182
Deleting QoS policies 183
Displaying QoS policy statistics 184
QoS agent 185
Displaying QoS agent configuration 185
Displaying policy class support 186
Displaying policy device identification 187
COPS overview 188
Displaying COPS capabilities 188
Displaying COPS current service configuration 189
Displaying COPS local configuration 191
Adding COPS local configuration data 192
Deleting COPS local configuration data 192
Displaying COPS retry setting 193
Displaying COPS statistics 194

Chapter 8
Setting up bridging 197

Base tab 197
Spanning Tree tab 198

Transparent tab 201
Forwarding tab 202

Chapter 9
Troubleshooting Device Manager 205

Topology tab 205
Topology Table tab 206

Chapter 10
RMON 209

Working with RMON information 209
Viewing statistics 210
Viewing history 211
Creating a history 212
Disabling history 214
Viewing RMON history statistics 214
Enabling Ethernet statistics gathering 216
Disabling Ethernet statistics gathering 218
Alarms 219
How RMON alarms work 219
Creating alarms 221
Alarm Manager example 222
Events 227
How events work 227
Viewing an event 227
Creating an event 229
Deleting an event 230
Log information 230
HP OpenView 231
Log only event bug 233

Chapter 11
Security parameters 235

General tab 235
SecurityList tab 238

Security, Insert SecurityList dialog box 238
AuthConfig tab 240
Security, Insert AuthConfig dialog box 241
AuthStatus tab 243
AuthViolation tab 245
Index 247

Figures

Figure 1 Device Manager window 28
Figure 2 Device Manager Properties dialog box 29
Figure 3 Open Device dialog box 31
Figure 4 Device view 33
Figure 5 Parts of the Device Manager window 34
Figure 6 Objects in the device view 36
Figure 7 MDA dialog box 38
Figure 8 Color port legend 40
Figure 9 Switch unit shortcut menu 40
Figure 10 Port shortcut menu 41
Figure 11 MDA shortcut menu 42
Figure 12 Line graph 45
Figure 13 Area graph 45
Figure 14 Bar graph 46
Figure 15 Pie graph 46
Figure 16 Interface statistics for a single port 47
Figure 17 Interface statistics for multiple ports 48
Figure 18 Statistics dialog box for a port 49
Figure 19 Globals tab 54
Figure 20 Edit IP dialog box — IP Address tab 55
Figure 21 Edit IP dialog box — ARP tab 56
Figure 22 Edit Chassis dialog box — System tab 58
Figure 23 Edit Chassis dialog box — Base Unit Info tab 61
Figure 24 Edit Chassis dialog box — Stack Info tab 62
Figure 25 Edit Chassis dialog box — Agent tab 65
Figure 26 Edit Chassis dialog box — SNMP tab 66
Figure 27 Edit Chassis dialog box — Trap Receivers tab 67
Figure 28 Chassis, Insert Trap Receive dialog box 68
Figure 29 Edit Chassis dialog box — Power Supply tab 69

Figure 30 Edit Chassis dialog box — Fan tab 70
Figure 31 Edit Chassis dialog box — CPU/Mem Utilization tab 71
Figure 32 Edit FileSystem dialog box 73
Figure 33 Graph Chassis dialog box — Chassis SNMP tab 76
Figure 34 Graph Chassis dialog box — IP tab 79
Figure 35 Graph Chassis dialog box — ICMP In tab 82
Figure 36 Graph Chassis dialog box — ICMP Out tab 83
Figure 37 Edit Port dialog box — Interface tab 87
Figure 38 Edit Port dialog box — VLAN tab 90
Figure 39 Edit Port dialog box — STG tab 91
Figure 40 Edit Port dialog box — EAPOL tab 94
Figure 41 Port dialog box — Port Interface tab 97
Figure 42 VLAN tab for multiple ports 99
Figure 43 EAPOL tab for multiple ports 101
Figure 44 Interface tab for graphing ports 104
Figure 45 Graph Port dialog box — Port Ethernet Errors tab 106
Figure 46 Graph Port dialog box — Bridge tab 109
Figure 47 Graph Port dialog box — RMON tab 111
Figure 48 Graph Port dialog box — EAPOL Stats tab 113
Figure 49 Graph Port dialog box — EAPOL Diag tab 115
Figure 50 MLT dialog box 120
Figure 51 PortMembers dialog box 121
Figure 52 MLT Statistics — Interface tab 122
Figure 53 MLT Statics dialog box — Ethernet Errors tab 124
Figure 54 VLAN Basic tab 128
Figure 55 VLAN, Insert Basic dialog box for a port-based VLANs 130
Figure 56 VLAN, Insert Basic dialog box for a protocol-based VLAN 132
Figure 57 VLAN, Insert Basic dialog box for a source MAC-based VLAN 134
Figure 58 VLAN dialog box 135
Figure 59 MAC, VLAN dialog box 135
Figure 60 Insert VLAN MAC dialog box 135
Figure 61 VLAN tab 137
Figure 62 Snoop tab 138
Figure 63 VLAN dialog box 139
Figure 64 STG Configuration tab 143

Figure 65 STG, Insert Configuration dialog box 145
Figure 66 STG Configuration tab - Highlighted configuration fields 147
Figure 67 Status tab 147
Figure 68 Ports tab 149
Figure 69 Interface Queue tab 152
Figure 70 Interface Group tab 153
Figure 71 Group Assignment dialog box 154
Figure 72 Insert Interface Group dialog box 156
Figure 73 Interface Assignments tab 157
Figure 74 Priority Q Assign tab 158
Figure 75 Priority mapping tab 159
Figure 76 DSCP Q Assign tab 160
Figure 77 DSCP mapping tab 161
Figure 78 IP filter tab 163
Figure 79 Insert IP filter dialog box 164
Figure 80 IP filter group tab 165
Figure 81 Insert IP filter group dialog box 166
Figure 82 Layer 2 filter tab 168
Figure 83 Insert Layer 2 filter dialog box 169
Figure 84 Layer 2 filter group tab 171
Figure 85 Insert Layer 2 filter group dialog box 172
Figure 86 QoS action tab 173
Figure 87 Insert QoS action dialog box 174
Figure 88 QoS meters tab 176
Figure 89 Insert QoS meters dialog box 177
Figure 90 QoS Shapers tab 178
Figure 91 Insert QoS shaper dialog box 180
Figure 92 QoS policies tab 181
Figure 93 Insert QoS policies dialog box 183
Figure 94 QoS policy statistics tab 184
Figure 95 configuration tab 186
Figure 96 Policy class support tab 187
Figure 97 Policy device identification tab 188
Figure 98 capabilities 189
Figure 99 Current 190

Figure 100 Configuration 191
Figure 101 Insert COPS configuration dialog box 192
Figure 102 Retry Setting 193
Figure 103 COPS statistics 194
Figure 104 Base tab 198
Figure 105 Spanning Tree tab 199
Figure 106 Transparent tab 201
Figure 107 Forwarding tab 203
Figure 108 Diagnostics dialog box — Topology tab 205
Figure 109 Diagnostics dialog box — Topology Table tab 206
Figure 110 Port dialog box — RMON tab 210
Figure 111 Port dialog box — RMON History tab 211
Figure 112 History tab 212
Figure 113 RMONControl, Insert History dialog box 213
Figure 114 Rmon History statistics 215
Figure 115 RMONControl dialog box — Ether Stats tab 217
Figure 116 RMONControl, Insert Ether Stats dialog box 217
Figure 117 RMONControl, Insert Ether Stats dialog box port list 217
Figure 118 How alarms fire 220
Figure 119 Alarm example — threshold less than 260 221
Figure 120 Alarm Manager dialog box 222
Figure 121 Alarm variable list 223
Figure 122 RMONAlarms dialog box — Alarms tab 225
Figure 123 RMONAlarms dialog box — Events tab 228
Figure 124 Insert Events dialog box 229
Figure 125 New event in the Events tab 229
Figure 126 Log tab 230
Figure 127 General tab 236
Figure 128 SecurityList tab 238
Figure 129 Security, Insert SecurityList dialog box 239
Figure 130 AuthConfig tab 240
Figure 131 Security, Insert AuthConfig dialog box 242
Figure 132 AuthStatus tab 244
Figure 133 AuthViolation tab 246

Tables

Table 1 Properties dialog box items 29
Table 2 SNMP community string default values 31
Table 3 Open Device dialog box fields 32
Table 4 Menu bar commands 34
Table 5 Toolbar buttons 35
Table 6 MDA dialog box fields 38
Table 7 MDA and MDA port colors 38
Table 8 Port color codes 39
Table 9 Switch unit shortcut menu commands 41
Table 10 Port shortcut menu commands 41
Table 11 Device Manager buttons 42
Table 12 Types of statistics 44
Table 13 Graph dialog box buttons 50
Table 14 Help file locations 52
Table 15 Globals tab items 54
Table 16 IP Addresses tab items 55
Table 17 ARP tab items 56
Table 18 System tab items 58
Table 19 Base Unit Info tab items 61
Table 20 Stack Info tab fields 63
Table 21 Agent tab fields 65
Table 22 SNMP tab fields 66
Table 23 Edit Chassis dialog box — Trap Receivers tab items 67
Table 24 Power Supply tab fields 69
Table 25 Fan tab fields 70
Table 26 CPU/Mem Utilization tab fields 71
Table 27 FileSystem dialog box items 73
Table 28 SNMP tab fields 76
Table 29 Chassis IP tab fields 79

Table 30 ICMP In tab fields 82
Table 31 ICMP Out tab fields 84
Table 32 Interface tab items for a single port 88
Table 33 VLAN tab items for a single port 90
Table 34 STG tab items for a single port 92
Table 35 EAPOL tab items for a single port 95
Table 36 Interface tab fields for multiple ports 97
Table 37 VLAN tab fields for multiple ports 100
Table 38 EAPOL tab fields for multiple ports 101
Table 39 Port Interface tab fields for multiple ports 104
Table 40 Ethernet Errors tab fields 107
Table 41 Bridge tab fields 110
Table 42 RMON tab fields 111
Table 43 EAPOL tab fields 114
Table 44 EAPOL Diag tab fields 116
Table 45 MLT dialog box fields 120
Table 46 Interface tab fields 122
Table 47 Ethernet Errors tab fields 125
Table 48 Basic tab fields 129
Table 49 Snoop tab fields 138
Table 50 VLAN dialog box fields 139
Table 51 Configuration tab fields 143
Table 52 STG, Insert Configuration tab fields 145
Table 53 Status tab fields 148
Table 54 Ports tab fields 150
Table 55 Interface Queue tab fields 152
Table 56 Interface Group tab fields 153
Table 57 Interface Assignments tab fields 157
Table 58 Priority Q Assign tab fields 159
Table 59 Priority mapping tab fields 160
Table 60 DSCP Q Assign tab fields 161
Table 61 DSCP mapping tab fields 162
Table 62 IP filter tab fields 163
Table 63 IP filter group tab fields 166
Table 64 Layer 2 filter tab fields 168

Table 65 Layer 2 filter group tab fields 171
Table 66 QoS action tab fields 173
Table 67 QoS meters tab fields 176
Table 68 QoS Shapers tab fields 179
Table 69 QoS policies tab fields 181
Table 70 QoS policy statistics tab fields 185
Table 71 configuration tab fields 186
Table 72 policy class support tab fields 187
Table 73 policy device identification tab fields 188
Table 74 Capabilities tab fields 189
Table 75 Current tab fields 190
Table 76 Configuration tab fields 191
Table 77 COPS Retry setting tab fields 193
Table 78 COPS statistics tab fields 195
Table 79 Base tab fields 198
Table 80 Spanning Tree tab fields 199
Table 81 Transparent tab items 202
Table 82 Forwarding tab fields 204
Table 83 Topology tab items 206
Table 84 Topology Table tab fields 207
Table 85 History tab fields 213
Table 86 Rmon History statistics tab fields 215
Table 87 Ether Stats tab fields 218
Table 88 RMON Insert Alarm dialog box fields 224
Table 89 Alarms tab fields 225
Table 90 Events tab fields 228
Table 91 Log tab fields 231
Table 92 General tab items 236
Table 93 SecurityList tab fields 238
Table 94 Security, Insert AuthConfig dialog box fields 239
Table 95 AuthConfig tab fields 241
Table 96 Security, Insert AuthConfig dialog box fields 242
Table 97 AuthStatus tab fields 244
Table 98 AuthViolation tab fields 246

Preface

Welcome to the Nortel Networks* Device Manager software, a set of graphical network management applications you can use to configure and manage the Nortel Networks Business Policy Switch 2000*. This guide provides information about using the features and capabilities of the Java*-based Device Manager graphical user interface (GUI) to perform network management operations for the switch.

Note: This version of Device Manager supports Business Policy Switch software version 2.0.

Before you begin

This guide is intended for network administrators with the following background:

- Basic knowledge of networks and Ethernet bridging
- Familiarity with networking concepts and terminology
- Basic knowledge of network topologies
- Familiarity with GUIs

Text conventions

This guide uses the following text conventions:

italic text	Indicates book titles.
separator (>)	Shows menu paths. Example: Protocols > IP identifies the IP option on the Protocols menu.

Related publications

For more information about using the Embedded Web Server and the BPS 2000, refer to the following publications:

- *Release Notes for the Business Policy Switch 2000 Software Version 2.0* (part number 210676-F)

  Documents important changes about the software and hardware that are not covered in other related publications.

- *Using the Business Policy Switch 2000 Version 2.0* (part number 208700-C)

  Describes how to use the BPS 2000.

- *Business Policy Switch 2000 Installation Instructions* (part number 209319-A*)*

  Describes how to install the BPS 2000.

- *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.0* (part number 212160-B)

  Describes how to use the Command Line Interface (CLI) to configure and manage the BPS 2000.

- *Configuring BayStack and Business Policy Switches with the Preside Network Configuration System* (part number 312061-B)

  Describes how to use the Preside Network Configuration System to configure and manage the BPS 2000.

- *Installing Media Dependent Adapters (MDA)s* (part number 302403-H)

  Describes how to install optional MDAs in your Business Policy Switch 2000.

- *Installing Gigabit Interface Converters and Small Form Factor Pluggable Interface Converters* (part number 312865-B)

  Describes how to install optional GBICs and SFF GBICs into the optional MDA in your Business Policy Switch 2000.

- *Installing Optivity Policy Services* (part number 306972-E Rev 00)

  Describes how to install Optivity Policy Services*.

- *Managing Policy Information in Optivity Policy Services*
(part number 306969-F Rev 00)

  Describes how to configure and manage Optivity Policy Services.

- *Release Notes for Optivity Policy Services Version 2.0.1*
(part number 306975-F Rev 00)

  Documents important Optivity Policy Services changes that are not covered in other related publications.

- *Task Map - Installing Optivity Policy Services Product Family*
(part number 306976-E Rev 00)

  Provides a quick map to installing Optivity Policy Services.

- *Known Anomalies for Optivity Policy Services Version 2.0*
(part number 306974-E Rev 00)

  Describes known anomalies with Optivity Policy Services.

These documents provide information about the Business Policy Switch including installation instructions and configuration settings.

You can print selected technical manuals and release notes free, directly from the Internet. Go to the www.nortelnetworks.com/documentation URL. Find the product for which you need documentation. (The product family for the BPS 2000 is Data and Internet.) Then locate the specific category and model or version for your hardware or software product. Use Adobe* Acrobat Reader* to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to Adobe Systems at the www.adobe.com URL to download a free copy of the Adobe Acrobat Reader.

How to get help

If you purchased a service contract for your Nortel Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact one of the following Nortel Networks Technical Solutions Centers:

Technical Solutions Center	Telephone
Europe, Middle East, and Africa	(33) (4) 92-966-968
North America	(800) 2LANWAN or (800) 252-6926
Asia Pacific	(61) (2) 9927-8800
China	(800) 810-5000

An Express Routing Code (ERC) is available for many Nortel Networks products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to the www12.nortelnetworks.com/ URL and click ERC at the bottom of the page.

Chapter 1
Device Manager basics

This chapter describes basic procedures for using the Device Manager software. The chapter includes the following information:

- Instructions to start Device Manager, set the Device Manager properties, and open a device (next)
- A summary of the Device Manager user interface features and how to use them (starting on page 33)
- Instructions to view statistics and display graphs (page 44)
- Instructions to use Device Manager to Telnet to a switch (page 50)
- Information about the trap log (page 51)
- Information about online Help (page 52)

Note: This version of Device Manager supports Business Policy Switch 2000 software version 2.0.

Starting Device Manager

➨ Do one of the following, depending upon your operating system environment:

- In a Microsoft® Windows® environment, from the Windows taskbar choose Start > Programs > Nortel Frame Switch Management Software > Device Manager.
- In a UNIX environment, you can run the Device Manager from the installation directory:

  ```
  ./JDM
  ```

  Or,

You can set up the environmental variable JDM_HOME. This allows you to run JDM from any directory if JDM_HOME is in the search path.

The initial Device Manager window opens (Figure)

Note: On startup, Device Manager performs a DNS lookup for the machine on which it is running. If the DNS lookup is slow or fails, the initial Device Manager window may take up to 30 seconds to open.

Figure 1 Device Manager window

Setting the Device Manager properties

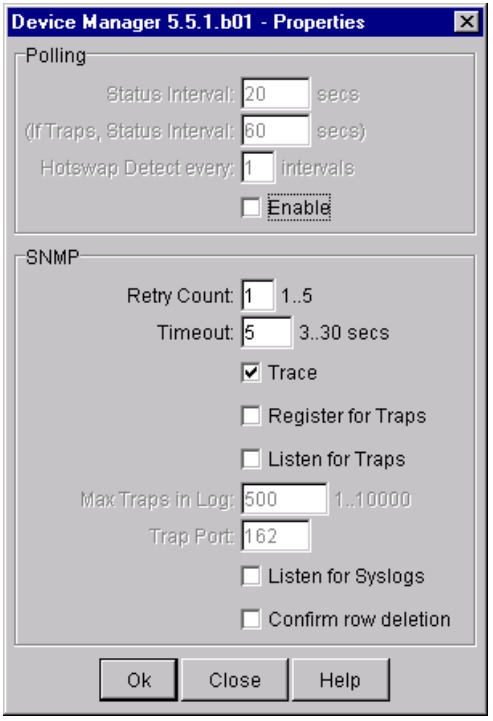
Device Manager communicates with the Using the Business Policy Switch 2000 using Simple Network Management Protocol (SNMP). The software is shipped with default values set for important communication parameters, such as the polling interval, timeout, and retry count. You may want to set the parameters before you open a device to manage.

To set the Device Manager properties:

1 Choose Device > Properties.

The Properties dialog box opens (Figure 2).

Figure 2 Device Manager Properties dialog box



2 Type information and select check boxes.

3 Click OK.

Table 1 describes the Properties dialog box items.

Table 1 Properties dialog box items

Area	Item	Description
Polling	Status Interval	Interval at which status information is gathered (default is 300 seconds). For a full stack, set this interval to 60 seconds.
	(If Traps, Status Interval:)	Interval at which statistics and status information are gathered when traps are enabled. The default is 300.

Table 1 Properties dialog box items (continued)

Area	Item	Description
	Hotswap Poll Interval	The interval at which Device Manager polls for module information. The default is 60 seconds.
	Enable	Enables (true) or disables (false) periodic polling of the device for updated status. If polling is disabled, the chassis status is updated only when you click Refresh on the Chassis tab.
SNMP	Retry Count	Number of times Device Manager sends the same polling request if a response is not returned to Device Manager. You may want to set this field to three or four.
	Timeout	Length of each retry of each polling waiting period. When you access the device through a slow link, you may want to increase the timeout interval and then change the Retransmission Strategy to superlinear.
	Trace	The trace field is used to enable and disable SNMP tracing. When Trace is selected, SNMP protocol data units (PDUs) are displayed in the Device > Log dialog box.
	Register for Traps	When selected (enabled), automatically registers to received traps when Device Manager is launched against a device.
	Listen for Traps	When selected (enabled), Device manager listens for traps from the device.
	Max Traps in Log	The specified number of traps that may exist in the trap log. The default is 500.
	Trap Port	Specifies the UDP port that Device Manager will listen on to receive SNMP traps.
	Confirm row deletion	A dialog box displays when checked, before deleting a row.

Opening a device

"Opening" a device displays the device view, a picture of the device. To open the device view, you must enter community strings that determine the access level granted to the device.

Table 2 shows the default access community strings for the Device Manager software.

Table 2 SNMP community string default values

Access level	Description
Read-only	public
Read-write	private
Read-write-all	secret

To display the device view:

1 Do one of the following:

- Choose Device > Open.
- Choose Device > Open Last, and select an IP address from the list.
- Click the folder icon in the Device Manager window.

- Press [Ctrl] + O.

  The Open Device dialog box opens (Figure 3).

Figure 3 Open Device dialog box

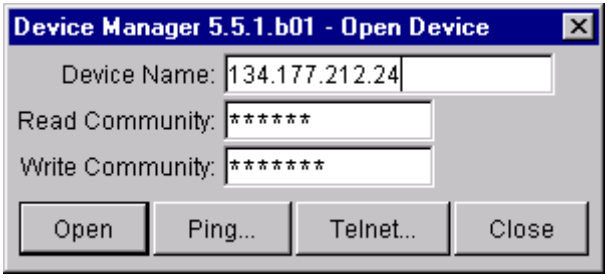


Table 3 describes the Open Device dialog box fields.

Table 3 Open Device dialog box fields

Field	Description
Device Name	Either an IP address or a DNS name for the device, entered by the user.
Read Community	SNMP read community string for the device. Default is `public` (displayed as ******). The entry is case-sensitive.
Write Community	SNMP write community string for the device. Default is `private` (displayed as *******).The entry is case-sensitive.

2 In the Device Name text box, type the DNS name or IP address of the device.

3 In the Read Community and Write Community text boxes, type the proper community strings.

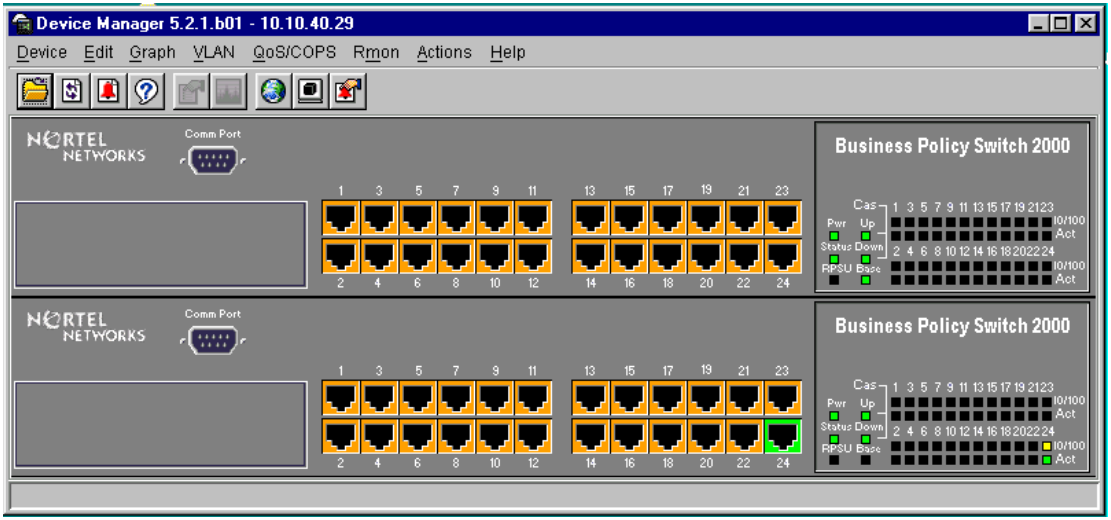
Note: To gain Read-Write-All access to a device in Device Manager, you must enter the Read-Write-All community string for both the Read Community and Write Community strings.

4 Click Open.

Device Manager automatically determines what version of software the selected device is running and displays the appropriate Device Manager dialog boxes.

The Device Manager window opens, showing a picture of the device (Figure 4) that represents the physical features of the device.

Figure 4 Device view

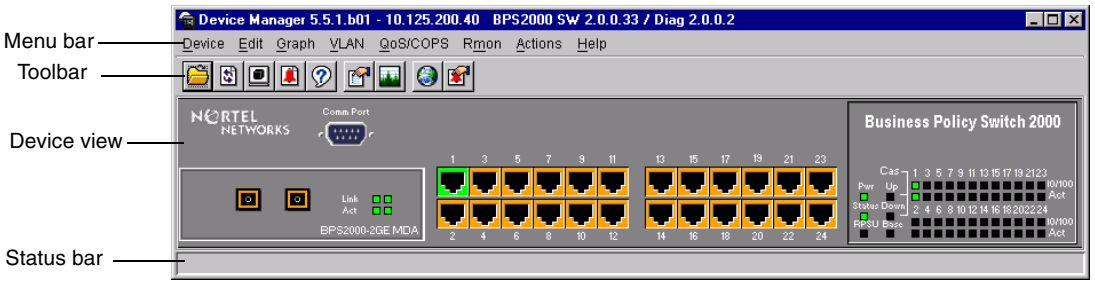


Device Manager window

The Device Manager window (Figure 5) has the following parts:

- Menu bar
- Toolbar
- Device view
- Status bar

Figure 5 Parts of the Device Manager window



Menu bar

Use the menu bar to set up and operate Device Manager (Table 4).

Table 4 Menu bar commands

Command	Description
Device	Opens the Open Device dialog box.
Edit	Opens edit dialog boxes for selected objects in the device view. This command also opens dialog boxes for managing files and running diagnostic tests.
Graph	Opens statistics dialog boxes for the selected object.
VLAN	Opens dialog boxes for managing VLANs, spanning tree groups (STGs), and Multi-Link Trunks.
QoS/COPS	Opens configuration and monitoring dialog boxes for Quality of Service (QoS), or Differentiated Services, and Common Open Policy Services (COPS).
Rmon	Opens RMON configuration and monitoring dialog boxes.
Actions	Provides quick opening of a Telnet session without going through other dialog boxes.
Help	Opens online Help topics for Device Manager and provides a legend for the port colors in the device view.

Toolbar

The toolbar contains buttons that provide quick access to commonly used commands and some additional actions.Table 5 describes the toolbar buttons.

Table 5 Toolbar buttons

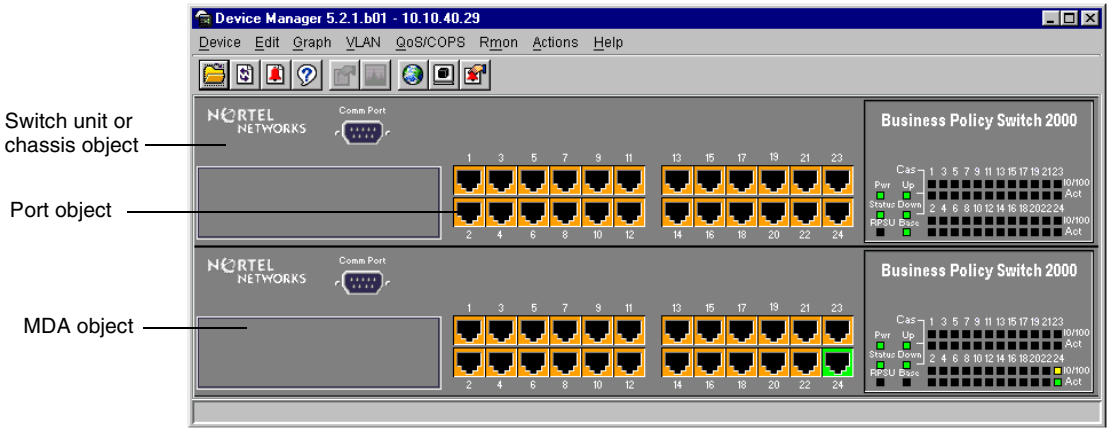
Button	Name	Description	Menu bar equivalent
	Open Device	Opens the Open Device dialog box.	Device > Open
	Refresh Device Status	Refreshes the device view information.	Device > Refresh Status
	Trap Log	Opens the trap log.	Device > Trap Log
	Help	Opens online Help in a Web browser.	Help > Device
	Edit Selected	Displays configuration data for the selected chassis object.	Edit > Unit Edit > Chassis Edit > Port
	Graph Selected	Opens statistics and graphing dialog boxes for the selected object	Graph > Chassis Graph > Port
	Globe	Opens a Web-based management session.	Actions > Open Home Page
	Telnet	Opens a Telnet session.	Actions > Telnet
	Alarm Manager	Opens the Rmon Alarm Manager.	Rmon > Alarm Manager

Device view

The device view allows you to determine at a glance the operating status of the various units and ports in your hardware configuration. You also use the device view to perform management tasks on specific objects.

Figure 6 shows the parts of a typical device view.

Figure 6 Objects in the device view


Switch unit or chassis object
Port object
MDA object
Device Manager 5.2.1.b01 - 10.10.40.29
Device Edit Graph VLAN QoS/COPS Rmon Actions Help
Business Policy Switch 2000
Business Policy Switch 2000

The following sections describe how you select and use objects in the device view:

- "Selecting objects," next
- "Selecting a single object" on page 36
- "Selecting multiple objects" on page 37
- "Viewing information about an MDA" on page 37
- "LEDs and ports" on page 39

Selecting objects

The types of objects contained in the device view are:

- A standalone switch (called a unit in the menus and dialog boxes)
- A switch stack (called a chassis in the menus and dialog boxes)
- A media dependent adapter (MDA) (called a unit in the menus and dialog boxes)
- A port

Selecting a single object

To select a single object:

➡ Click the edge of the object.

The object is outlined in yellow, indicating that it is selected. Subsequent activities in Device Manager refer to the selected object.

Selecting multiple objects

To select multiple objects of the same type (such as ports or switches of the same type):

➡ Do one of the following:

- For a block of contiguous ports, drag to select the group of ports.
- For multiple ports, MDAs, or switches in the stack, [Ctrl]-click on the objects.

Note: In a switch stack that contains Business Policy Switches and BayStack switches, you can select only one type of switch at a time.

To select all the ports in a standalone switch or in a switch stack:

➡ Choose Edit > Select > Ports.

To select all the "units" (switches and MDAs, but not ports):

➡ Choose Edit > Select > Units.

To select an entire stack:

➡ Choose Edit > Select > Chassis.

Viewing information about an MDA

To view information about an MDA:

1 Select the MDA.

2 Choose Edit > Unit.

The Edit > Unit dialog box opens for the MDA.

The Edit > Unit dialog box describes the MDA installed in the switch (Figure 7).

Figure 7 MDA dialog box

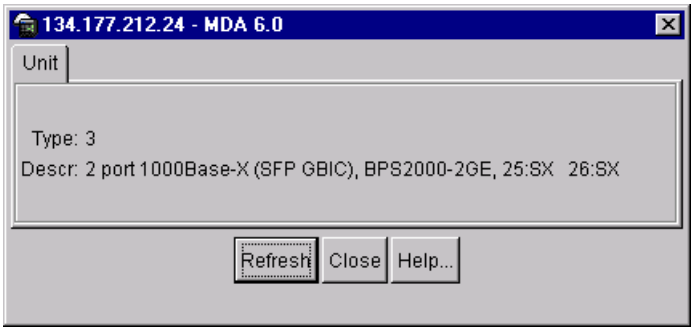


Table 7 describes the MDA dialog box fields.

Table 6 MDA dialog box fields

Field	Description
Type	Type of component or subcomponent installed in the Business Policy Switch 2000.
Descr	Description of the component or subcomponent installed in the Business Policy Switch 2000. If not available, the value is a zero length string

Media dependent adapters and port conventions

The conventions on the graphical representation of the switch are different from the actual switch. The colors in the graphical representation of the MDA and ports are color-coded to provide port status.

Table 7 describes the colors in the graphical representation of the MDA and its ports.

Table 7 MDA and MDA port colors

Color	Description
Green	The module/port is operating.
Red	The module/port is present, but not operating.
Dark blue	Port is being tested.

Table 7 MDA and MDA port colors (continued)

Color	Description
Dark red	Port has been manually disabled.
Orange	Port has no link.

A blinking LED on an MDA is not indicated in the graphical representation of the switch.

For a full description of switch LEDs, refer to the respective switch user manuals.

LEDs and ports

The color of LEDs in the device view is the same as the colors of the LEDs on the physical switch. However, the device view does not show blinking activity of the LEDs.

For a full description of the LEDs for the Business Policy Switch, refer to *Using the Business Policy Switch 2000*.

The ports on the device view are color coded to show port status.

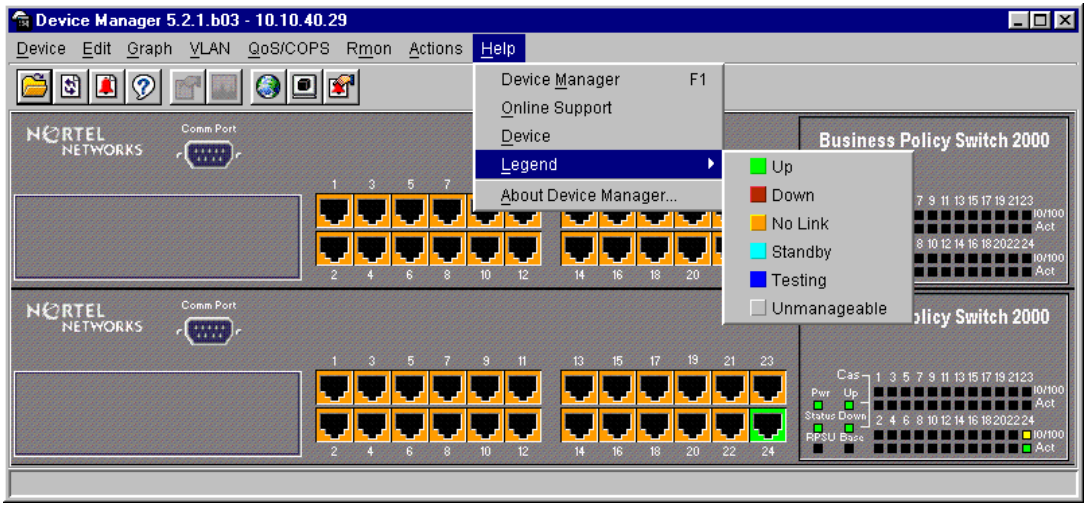
Table 8 shows the status assigned to each color.

Table 8 Port color codes

Color	Description
Green	Port is operating.
Red	Port has been manually disabled.
Orange	Port has no link.
Light Blue	Port is in standby mode.
Dark Blue	Port is being tested.
Gray	Port is unmanageable.

In addition, the Help menu provides a legend that identifies the port colors and their meanings.

Figure 8 Color port legend



Shortcut menus

Each object in the device view has a shortcut menu that opens when you right-click a selected object. The switch shortcut menu provides access to basic hardware information about the switch and to the graphing dialog boxes for the switch.

Figure 9 Switch unit shortcut menu

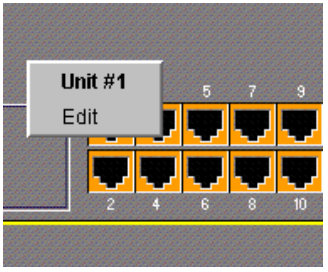


Table 9 describes the commands on the switch unit shortcut menu.

Table 9 Switch unit shortcut menu commands

Command	Description
Edit	Opens a read-only dialog box that provides basic hardware information about the switch.
Graph	Opens a dialog box that displays statistics for the switch and allows you to display the statistics as a graph.

The port shortcut menu provides a faster path for editing and graphing a single port; however, you can access the same options using the menu bar or the toolbar.

Figure 10 Port shortcut menu

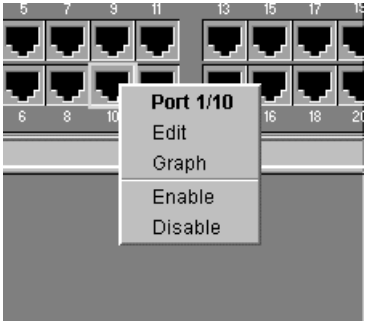


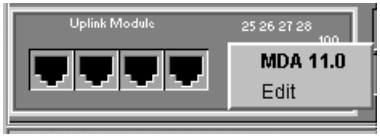
Table 10 describes the commands on the port shortcut menu.

Table 10 Port shortcut menu commands

Command	Descriptions
Edit	Opens a dialog box that allows you to set operating parameters for the port.
Graph	Opens a dialog box that displays statistics for the port and allows you to display the statistics as a graph.
Enable	Administratively brings a port up.
Disable	Administratively shuts down a port. The color of the port changes to red in the device view.

The MDA shortcut menu contains a single command, Edit, that opens a read-only dialog box with basic hardware information about the MDA.

Figure 11 MDA shortcut menu



Status bar

The status bar displays error and informational messages from the software application. These messages are not related to the device being managed.

Using the buttons in Device Manager dialog boxes

Table 11 describes buttons in Device Manager dialog boxes. Not all buttons appear in all dialog boxes.

Table 11 Device Manager buttons

Button	Name	Description
	Insert	Opens a dialog box to create a new entry for a table; then from the dialog box, inserts the new entry in the table.
	Copy	Copies selected cells from a table.
	Paste	Pastes copied values to a currently selected table cell.
	Reset Changes	Causes changed (but not applied) fields to revert to their previous values.
	Print Table or Print Graph	Prints a table or graph.

Table 11 Device Manager buttons (continued)

Button	Name	Description
	Stop	Stops the current action (compiling, saving, and so forth). If you are updating or compiling a large data table, the Refresh button changes to a Stop button while this action is taking place. Clicking the Stop button interrupts the polling process.
	Export Data	Exports information to a file you specify. You can then import this file into a text editor or spreadsheet for further analysis.

Editing objects

You can edit objects and values in the Device Manager device view in the following ways:

- Select an object and, on the toolbar, click the Edit Selected button.

  The edit dialog box opens for that object.

- From a switch or port shortcut menu, choose Edit. The edit dialog box opens for that object.

When you change the value in a box, the changed value is shown in **bold**. However, changes are not applied to the running configuration until you click Apply.

Note: Many dialog boxes contain a Refresh button. After you apply changes to fields, click Refresh to display the new information in the dialog box.

Working with statistics and graphs

Device Manager tracks a wide range of statistics for each switch, the stack (chassis), and each port. You can view and graph statistics for a single object or multiple objects. For information about the statistics tracked for the switch and ports, refer to "Statistics for single and multiple objects" on page 47 and "Graphing chassis statistics" on page 74.

This section describes the types of statistics and graphs available, the graph dialog boxes, and the procedure for creating a graph.

Types of statistics

The data tables in the statistics dialog boxes list the counters, or categories of statistics being gathered, for the specified object. For example, the categories for ports include Interface, Ethernet Errors, Bridge, and Rmon. Each category can be associated with six types of statistics.

Table 12 describes the types of statistics shown in the statistics dialog boxes.

Table 12 Types of statistics

Statistic	Description
AbsoluteValue	The total count since the last time counters were reset. A system reboot resets all counters.
Cumulative	The total count since the statistics window was first opened. The elapsed time for the cumulative counter is shown at the bottom of the graph window.
Average/sec	The cumulative count per polling interval.
Minimum/sec	The minimum average for the counter per polling interval.
Maximum/sec	The maximum average for the counter per polling interval.
LastVal/sec	The average for the counter during the previous polling interval.

Types of graphs

With Device Manager, you can create line, area, bar, and pie graphs. Figure 12, Figure 13, Figure 14, and Figure 15 illustrate the different graph styles, respectively.

Figure 12 Line graph

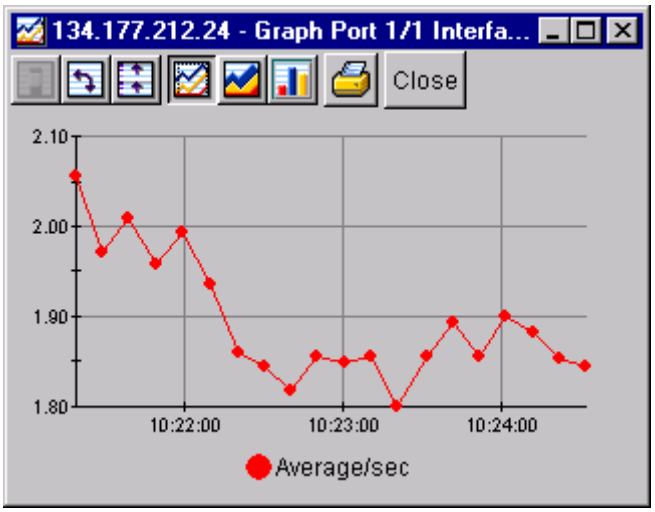


Figure 13 Area graph

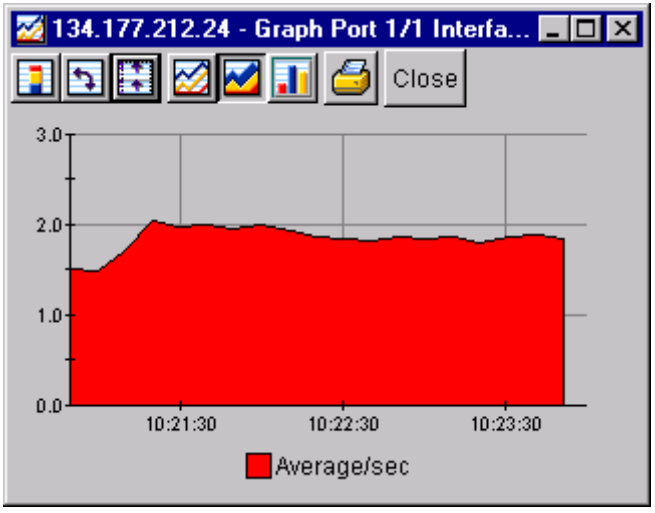


Figure 14 Bar graph

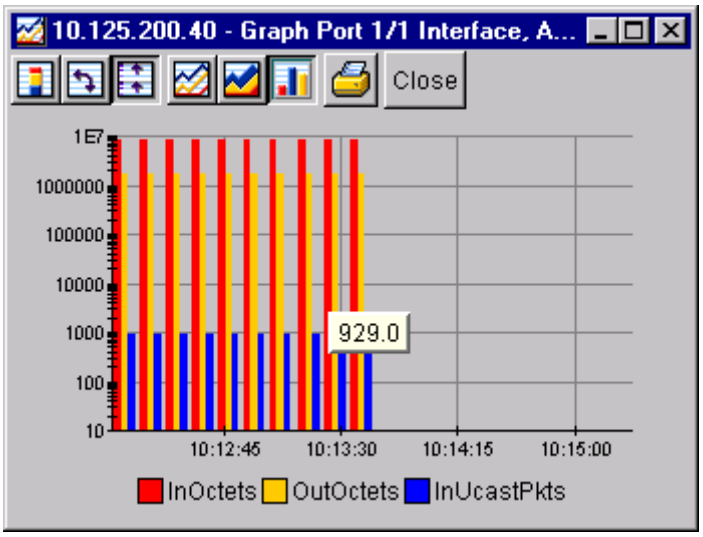
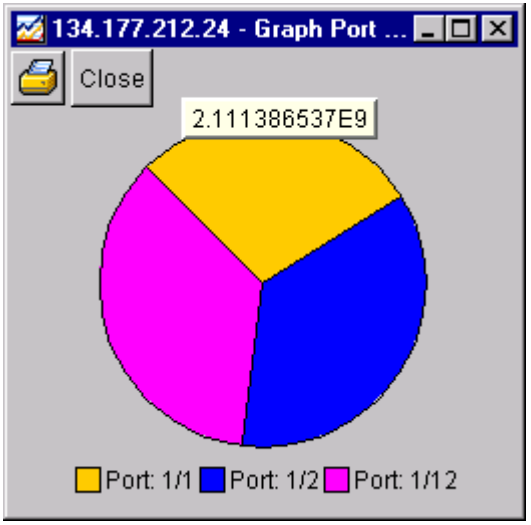


Figure 15 Pie graph

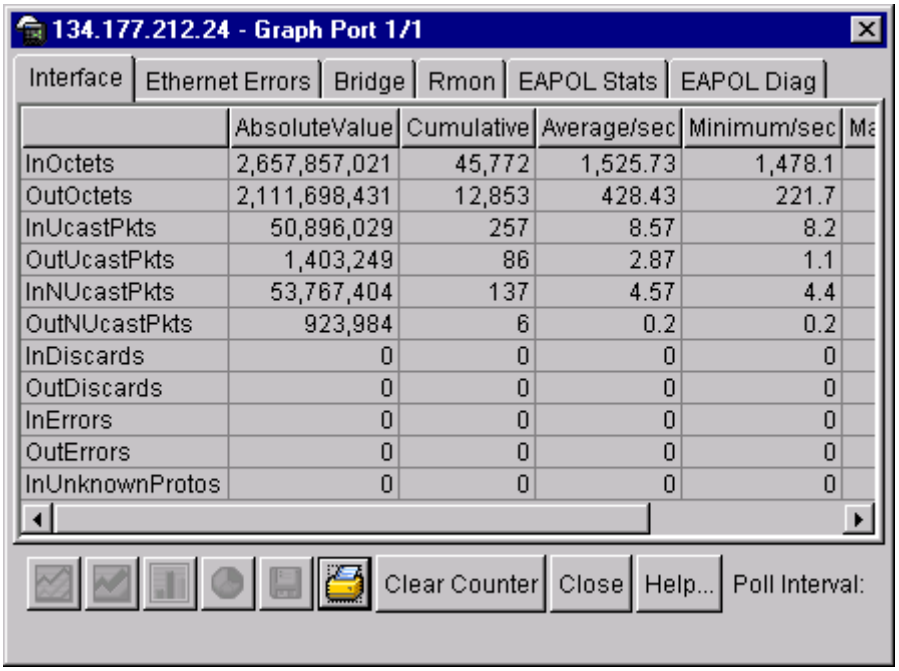


Statistics for single and multiple objects

The statistics dialog box displays statistics for a selected object.

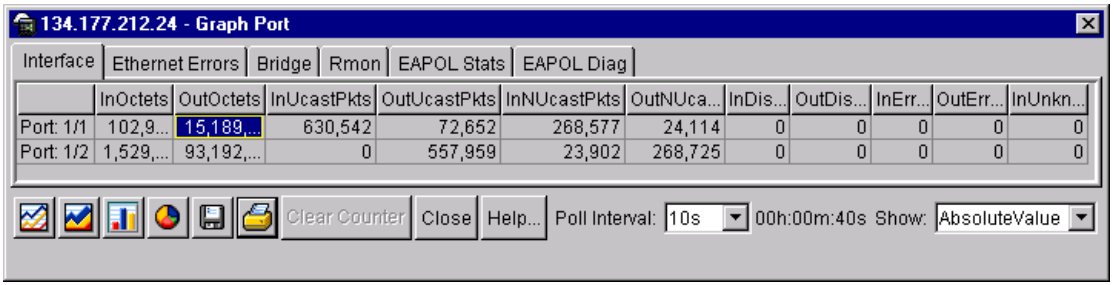
The dialog box for a single object shows all six types of statistics for each counter (Figure 16).

Figure 16 Interface statistics for a single port



The statistics dialog box for multiple objects shows a single type of statistics (Table 12) for the selected objects. For example, Figure 17 shows LastValue statistics for the selected ports.

Figure 17 Interface statistics for multiple ports



To change the type of statistics displayed, select a different type from the show list at the bottom of the dialog box.

The statistics are updated based on the poll interval shown at the bottom of the dialog box. You can select a different polling interval.

Buttons for bar, pie, and line graphs are located at the bottom of a statistics dialog box.

See "Viewing statistics as graphs," next for instructions on using these buttons.

You can export the statistics to a tab-separated file format and import the file into other applications. To export the information, use the Export Data button below the table.

Viewing statistics as graphs

To create a graph for an object:

1 Select the object or objects to be graphed

See "Selecting objects" on page 36 for more information.

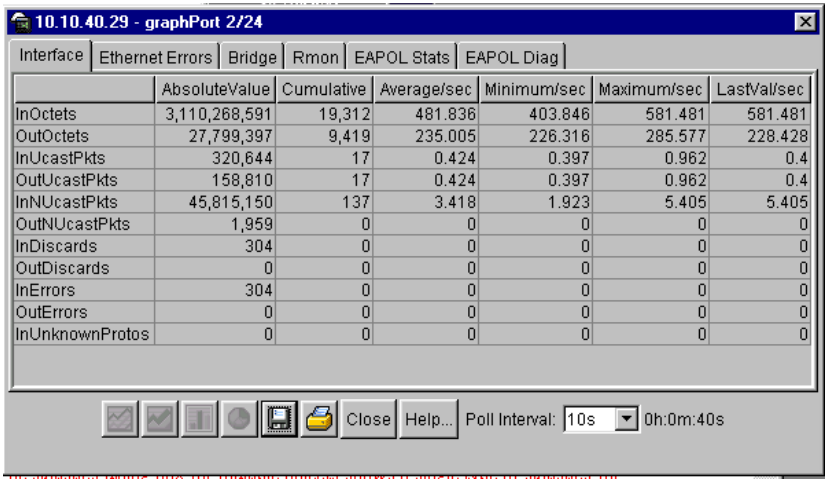
2 Do one of the following:

- On the toolbar, click Graph Selected.

- From the shortcut menu for the object, choose Graph.
- From the main menu, choose Graph > Chassis or Graph > Port.

A statistics dialog box opens with tabs for different categories of statistics for the selected object (Figure 18).

Figure 18 Statistics dialog box for a port


10.10.40.29 - graphPort 2/24
Interface
Ethernet Errors
Bridge
Rmon
EAPOL Stats
EAPOL Diag
AbsoluteValue Cumulative Average/sec Minimum/sec Maximum/sec LastVal/sec
InOctets 3,110,268,591 19,312 481.836 403.846 581.481 581.481
OutOctets 27,799,397 9,419 235.005 226.316 285.577 228.428
InUcastPkts 320,644 17 0.424 0.397 0.962 0.4
OutUcastPkts 158,810 17 0.424 0.397 0.962 0.4
InNUcastPkts 45,815,150 137 3.418 1.923 5.405 5.405
OutNUcastPkts 1,959 0 0 0 0 0
InDiscards 304 0 0 0 0 0
OutDiscards 0 0 0 0 0 0
InErrors 304 0 0 0 0 0
OutErrors 0 0 0 0 0 0
InUnknownProtos 0 0 0 0 0 0
Close
Help...
Poll Interval:
10s
0h:0m:40s

3 Select a tab for the group of statistics you want to view.

4 On the displayed data table, drag to select the cells you want to graph. (They must be in the same row or column.)

5 Click one of the graph buttons at the bottom of the dialog box

See "Types of graphs" on page 44 for more information.

A graph dialog box opens for the selected graph type.

6 To print a copy of the graph, click Print.

Buttons at the top of the graph dialog boxes for line, area, and bar graphs allow you to change the orientation of the graph, change the scale, or change the graph type.

Table 13 describes the buttons in the graph dialog boxes.

Table 13 Graph dialog box buttons

Button	Name	Description
	Stacked	"Stacks" data quantities instead of displaying them side-by-side.
	Horizontal	Rotates the graph 90 degrees.
	Log Scale	Changes the scale of the x-axis (of an unrotated graph) from numeric to logarithmic.
	Line Chart	Converts an area graph or bar graph to a line graph.
	Area Chart	Converts a line graph or bar graph to an area graph.
	Bar Chart	Converts a line graph or area graph to a bar graph.

Telneting to a switch

From Device Manager, you can initiate a Telnet session to the console interface for the switch or stack you are currently accessing.

To Telnet to a switch:

➨ Do one of the following:

- From the Device Manager main menu, choose Actions > Telnet.
- On the toolbar, click the Telnet button.

A Telnet window to the switch opens.

Trap log

You can configure a Business Policy Switch to send SNMP generic traps. When Device Manager is running, any traps received are recorded in the trap log. You set the maximum number of entries in the trap log using the Properties window (Figure 2). The default number of trap log entries is 500.

To view the trap log:

➨ Do one of the following:

- On the toolbar, click the Trap Log button.

- From the Device Manager Main Menu, choose Device > Trap Log.

Note: When you operate Device Manager from a UNIX platform, you must be logged in as root in order to receive traps.

Device Manager receives traps on port 162. If this port is being used by another application, you will not be able to view the trap log until the other application is disabled and Device Manager is restarted.

By default, traps are sent in SNMP V2c format. However, if you are using an older network management system (NMS), one that supports only SNMP V1 traps (HP OpenView), you can specify that the traps be sent in V1 format.

Management stations operating with Device Manager are automatically added to trap receivers.

For more information about traps and trap receivers, refer to *Using the Business Policy Switch 2000*.

Online Help

Online Help in Device Manager is context-sensitive. You use a Web browser to display online Help. The Web browser should launch automatically when you click the Help button. If the Help topic you are accessing is not displayed in your browser, exit the existing browser session and click the Help button again.

If, for some reason, the Web browser does not launch, the default locations of the Help files are the directories listed in Table 14.

Table 14 Help file locations

Platform	Default path
Windows 95, Windows 98, or Windows NT	*c:\Program files\JDM\DM\help\dmhelp.html*
UNIX	*UNIX directory/JDM/help/dmhelp.html*

Chapter 2
Configuring and graphing the switch

The first three sections of this chapter describe how you can use Device Manager to configure your switch. The last section describes how to use Device Manager to graph switch statistics.

Viewing switch IP information

You can view the switch IP information using the IP dialog box.

To open the IP dialog box:

➨ From the Device Manager main menu, choose Edit > IP.

The Edit IP dialog box opens (Figure 19) with the Globals tab displayed.

Globals tab

To open the Globals tab:

➨ From the Device Manager main menu, choose Edit > IP.

The IP dialog box opens (Figure 19) with the Globals tab displayed.

Figure 19 Globals tab

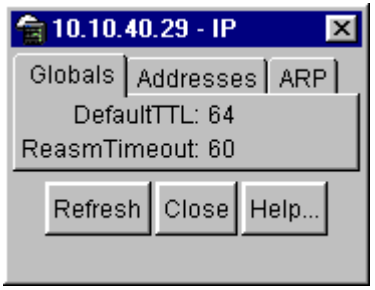


Table 15 describes the Globals tab items.

Table 15 Globals tab items

Item and MIB association	Description
DefaultTTL	Default value inserted into the Time-To-Live field of the IP header of datagrams originated at this entity, whenever a TTL value is not supplied by the transport layer protocol. Default value is 16.
ReasmTimeout	Maximum number of seconds that received fragments are held while they are awaiting reassembly at this entity. Default value is 5.

Addresses tab

The Addresses tab shows the IP address information for the device.

To open the Addresses tab:

1 From the Device Manager main menu, choose Edit > IP.

The IP dialog box opens with the Globals tab displayed (Figure 19).

2 Click the Addresses tab.

The Addresses tab opens (Figure 20).

Figure 20 Edit IP dialog box — IP Address tab

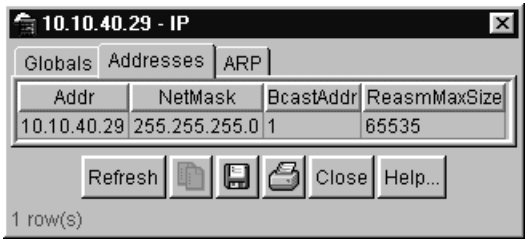


Table 16 describes the IP Address tab items.

Table 16 IP Addresses tab items

Item	Description
Addr	The device IP address.
NetMask	The subnet mask address.
BcastAddr	The IP broadcast address used.
ReasmMaxSize	The size of the largest IP datagram that this entity can reassemble from incoming IP fragmented datagrams received on this interface.

ARP tab

The Address Resolution Protocol (ARP) tab shows the MAC addresses and the associated IP addresses for the switch.

To open the ARP tab:

1 From the Device Manager main menu, choose Edit > IP.

The IP dialog box opens with the Globals tab displayed (Figure 19).

2 Click the ARP tab.

The ARP tab opens (Figure 21).

Figure 21 Edit IP dialog box — ARP tab

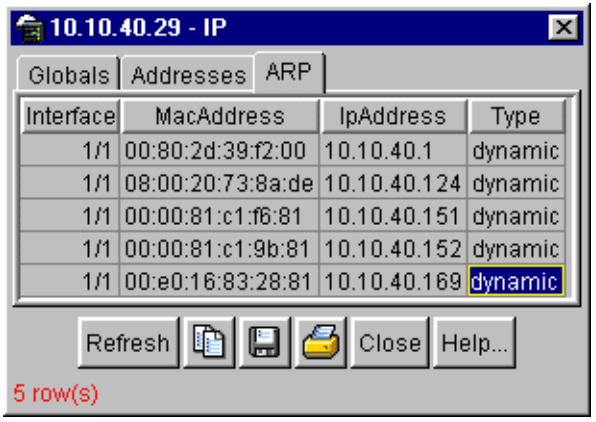


Table 17 describes the ARP tab items.

Table 17 ARP tab items

Item	Description
Interface	The device unit number.
MacAddress	The unique hardware address of the device.
IpAddress	The Internet Protocol address of the device used to represent a point of attachment in a TCP/IP internetwork.
Type	The type of mapping.

Editing the chassis configuration

You can edit a chassis configuration from the Edit Chassis dialog box (Figure 22).

To open the Chassis dialog box:

1 Select the chassis.

2 Do *one* of the following:

- From the shortcut menu, choose Edit.
- From the Device Manager main menu, choose Edit > Chassis.

- On the toolbar, click Edit.

The following sections provide a description of the tabs in the Edit > Chassis dialog box and details about each item on the tab:

- "System tab," next
- "Base Unit Info tab" on page 60
- "Stack Info tab" on page 62
- "Agent tab" on page 64
- "SNMP tab" on page 65
- "Trap Receivers tab" on page 67
- "Power Supply tab" on page 68
- "Fan tab" on page 69
- "CPU/Mem Utilization tab" on page 71

System tab

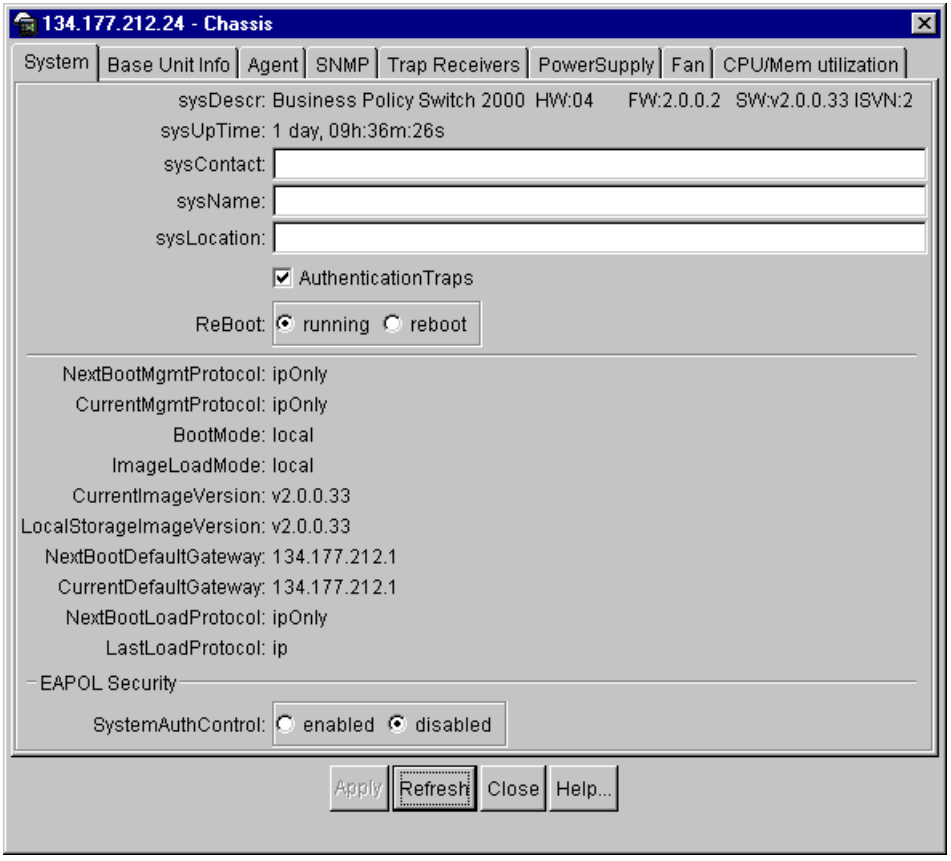
Use the System tab to specify, among other things, tracking information for a device and device descriptions.

To open the System tab:

1. Select the chassis.
2. From the shortcut menu, choose Edit > Chassis.

   The Chassis dialog box opens with the System tab displayed (Figure 22).

Figure 22 Edit Chassis dialog box — System tab



Note: The chassis keeps track of the elapsed time and calculates the time and date using the system clock of the Device Manager machine as a reference.

Table 18 describes the System tab items.

Table 18 System tab items

Item	Description
sysDescr	A description of the device.
sysUpTime	The time since the system was last booted.

Table 18 System tab items (continued)

Item	Description
sysContact	Type the contact information (in this case, an e-mail address) for the system administrator.
sysName	Type the name of this device.
sysLocation	Type the physical location of this device.
AuthenticationTraps	Click enable or disable. When you select enabled, SNMP traps are sent to trap receivers for all SNMP access authentication. When you select disabled, no traps are received. To view traps, click the Trap toolbar button.
Reboot	Action object to reboot the agent. Reset — initiates a hardware reset. The agent does best efforts to return a response before the action occurs. If any of the combined download actions are requested, neither action occurs until the expiration of s5AgInfoScheduleBootTime, if set.
NextBootMgmtProtocol	The transport protocol(s) to use after the next boot of the agent.
CurrentMgmtProtocol	The current transport protocol(s) that the agent supports.
BootMode	The source from which to load the initial protocol configuration information to boot the switch the next time, local (from the switch), or net (over the network), or none.
ImageLoadMode	The source from which to load the agent image at the next boot.
CurrentImageVersion	The version number of the agent image that is currently used on the switch.
LocalStorageImageVersion	The version number of the agent image that is stored in flash memory on the switch.
NextBootDefaultGateway	The IP address of the default gateway for the agent to use after the next time the switch is booted.
CurrentDefaultGateway	The IP address of the default gateway that is currently in use.

Table 18 System tab items (continued)

Item	Description
NextBootLoadProtocol	The transport protocol to be used by the agent to load the configuration information and the image at the next boot.
LastLoadProtocol	The transport protocol last used to load the image and configuration information on the switch.
EAPOL Security SystemAuthControl	SystemAuthControl field enables port access control in the system.

Base Unit Info tab

The Base Unit Info tab provides read-only information about the operating status of the hardware and whether or not the default factory settings are being used.

To open the Base Unit Info tab:

1. Select the chassis.
2. From the shortcut menu, choose Edit > Chassis.

   The Chassis dialog box opens with the System tab displayed (Figure 22).

3. Click the Base Unit Info tab.

   The Base Unit Info tab opens (Figure 23).

   In a stack environment, if the base unit number does not begin with the number one, the information will not be displayed. Use the console interface and the Web-based management interface to change your base unit number. For detailed information, refer to *Using the Business Policy Switch 2000* and *Using Web-based Management for the Business Policy Switch 2000*.

Figure 23 Edit Chassis dialog box — Base Unit Info tab

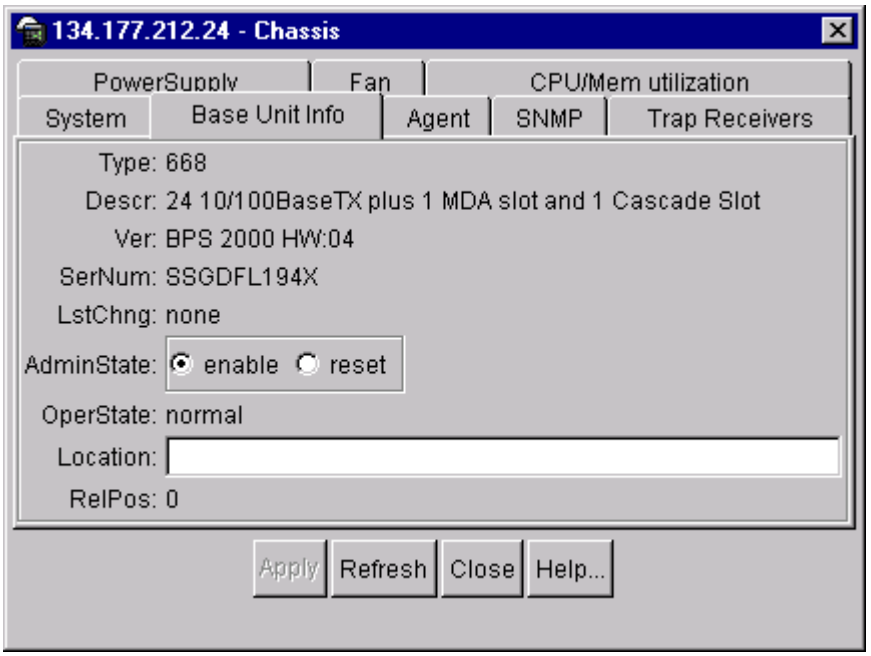


Table 19 describes the Base Unit Info tab items.

Table 19 Base Unit Info tab items

Item	Description
Type	The switch type.
Descr	A description of the switch hardware, including number of ports and transmission speed.
Ver	The switch hardware version number.
SerNum	The switch serial number.
LstChng	The value of sysUpTime at the time the interface entered its current operational state. If the current state was entered prior to the last reinitialization of the local network management subsystem, the value is zero.
AdminState	Administrative state of the switch. Select either `enable` or `reset`. **Note**: In a stack configuration, `Reset` only resets the base unit.
OperState	The operational state of the switch.

Table 19 Base Unit Info tab items (continued)

Item	Description
Location	Type the physical location of the switch.
RelPos	The relative position of the switch.

Stack Info tab

Like the Base Unit Info tab, the Stack Info tab provides read-only information about the operating status of the *stacked* switches and whether or not the default factory settings are being used. This tab is enabled for a stack of Business Policy Switches or a mixed stack of BayStack 450 and 410s and Business Policy Switches.

To open the Stack Info tab:

1. Select the chassis.
2. From the shortcut menu, choose Edit > Chassis.

   The Chassis dialog box opens with the System tab displayed (Figure 22).

3. Click the Stack Info tab.

   The Stack Info tab opens (Figure 24).

Figure 24 Edit Chassis dialog box — Stack Info tab

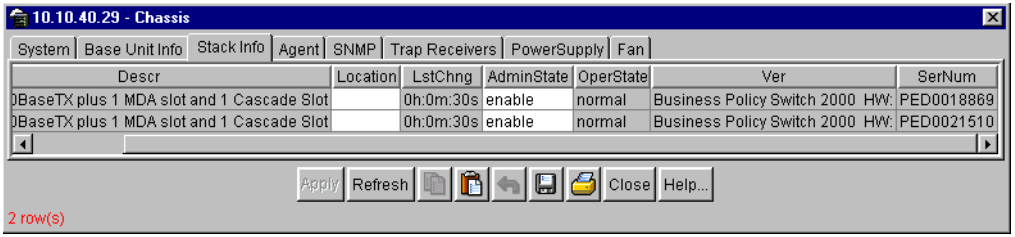


Table 20 describes the Stack Info tab fields.

Table 20 Stack Info tab fields

Field	Description
Descr	A description of the component or subcomponent. If not available, the value is a zero length string.
Location	The geographic location of a component in a system modeled as a chassis, but possibly physically implemented with geographically separate devices connected together to exchange managment information. Chassis modeled in this manner are sometimes referred to as virtual chassis. An example value is: '4th flr wiring closet in blg A'. Notes: 1. This object is applicable only to components that can be found in either the Board or Unit groups. If the information is unavailable, for example, the chassis is not modeling a virtual chassis or component is not in Board or Unit group, the value is a zero length string. 2. If this object is applicable and is not assigned a value through a SNMP SET PDU when the row is created, the value will default to the value of the object s5ChasComSerNum.
LstChng	The value of sysUpTime when it was detected that the component/ sub-component was added to the chassis. If this has not occurred since the cold/warm start of the agent, then the value is zero.
AdminState	The state of the component or subcomponent. The values that are read-only are: • other — currently in some other state • notAvail — actual value is not available The possible values that can be read and written are: 1. disable—disables operation 2. enable—enables operation 3. reset—resets component 4. test—starts self test of component, with the result to be normal, warning, nonFatalErr, or fatalErr in object s5ChasComOperState The allowable (and meaningful) values are determined by the component type.

Table 20 Stack Info tab fields (continued)

Field	Description
OperState	The current operational state of the component. The possible values are: • other—some other state • notAvail—state not available • removed—component removed • disabled—operation disabled • normal—normal operation • resetInProg—reset in progress • testing—doing a self test • warning—operating at warning level • nonFatalErr—operating at error level • fatalErr—error stopped operation The allowable (and meaningful) values are determined by the component type.
Ver	The version number of the component or subcomponent. If not available, the value is a zero length string.
SerNum	The serial number of the component or subcomponent. If not available, the value is a zero length string.

Agent tab

The Agent tab provides read-only information about the addresses that the agent software uses to identify the switch.

To open the Agent tab:

1 Select the chassis.

2 From the shortcut menu, choose Edit > Chassis.

The Chassis dialog box opens (Figure 22) with the System tab displayed.

3 Click the Agent tab.

The Agent tab opens (Figure 25).

Figure 25 Edit Chassis dialog box — Agent tab

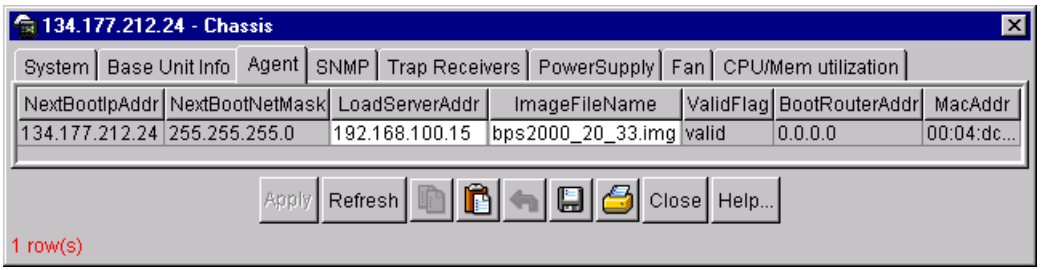


Table 21 describes the Agent tab fields.

Table 21 Agent tab fields

Item	Description
NextBootpAddr	The IP address of the BootP server to be used the next time the switch is booted.
NextBootNetMask	The subnet mask to be used the next time the switch is booted.
LoadServerAddr	The IP address of the server from which the device loads the image file.
ImageFileName	The name of the image file.
ValidFlag	Indicates if the configuration and/or image file(s) were downloaded from this interface and if the file names have not been changed.
BootRouterAddr	The IP address of the boot router for the configuration file and/or the image file.
MacAddr	The switch's MAC address.

SNMP tab

The SNMP tab provides read-only information about the addresses that the agent software uses to identify the switch.

To open the SNMP tab:

1. Select the chassis.
2. From the shortcut menu, choose Edit > Chassis.

   The Chassis dialog box opens (Figure 22) with the System tab displayed.

3 Click the SNMP tab.

The SNMP tab opens (Figure 26).

Figure 26 Edit Chassis dialog box — SNMP tab

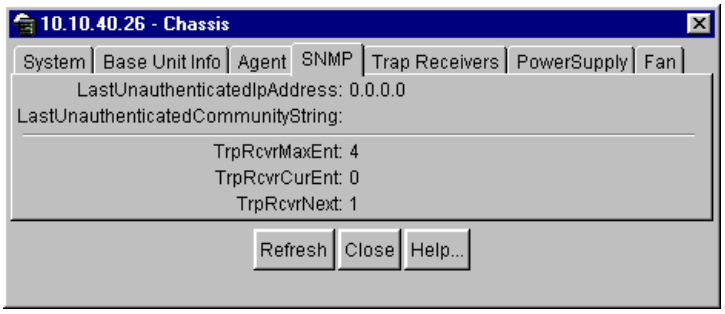


Table 22 describes the SNMP Info tab fields.

Table 22 SNMP tab fields

Field	Description
LastUnauthenticatedIpAddress	The last IP address that was not authenticated by the device.
LastUnauthenticatedCommunityString	The last community string that was not authenticated by the device.
TrpRcvrMaxEnt	The maximum number of trap receiver entries.
TrpRcvrCurEnt	The current number of trap receiver entries.
TrpRcvrNext	The next trap receiver entry to be created.

Trap Receivers tab

The Trap Receivers tab lists the devices that will receive SNMP traps from the Business Policy Switch switch.

When Device Manager opens a device, it automatically adds the device to the Trap Receivers list.

To open the Trap Receivers tab:

1 Right-click the chassis and choose Edit > Chassis from the shortcut menu.

The Chassis dialog box opens (Figure 22) with the System tab displayed.

2 Click the Trap Receivers tab.

The Trap Receivers tab opens (Figure 27).

Figure 27 Edit Chassis dialog box — Trap Receivers tab

Table 23 describes the Trap Receivers tab items.

Table 23 Edit Chassis dialog box — Trap Receivers tab items

Item	Description
NetAddr	The address (or DNS hostname) for the trap receiver.
Community	Community string used for trap messages to this trap receiver.

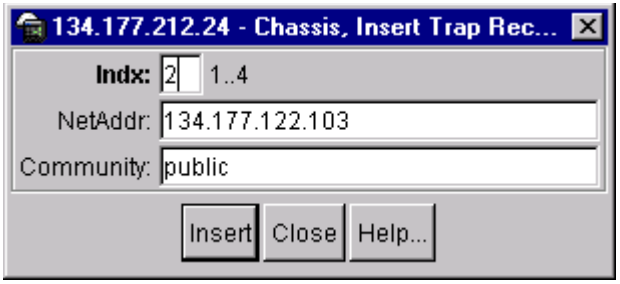
Editing network traps

To edit the network traps table:

1 In the Trap Receivers tab (Figure 27), click Insert.

The Chassis, Insert Trap Receive dialog box opens (Figure 28).

Figure 28 Chassis, Insert Trap Receive dialog box



2 Type the Index, NetAddr, and the Community information.

Note: Refer to Table 23 for a description of the Chassis, Insert Trap Receivers dialog box items.

3 Click Insert.

Power Supply tab

The Power Supply tab provides read-only information about the operating status of the switch power supplies.

To open the PowerSupply tab:

1 Select the chassis.

2 From the shortcut menu, choose Edit > Chassis.

The Chassis dialog box opens (Figure 22) with the System tab displayed.

3 Click the PowerSupply tab.

The PowerSupply tab opens (Figure 29).

Figure 29 Edit Chassis dialog box — Power Supply tab

Table 24 describes the Power Supply tab fields.

Table 24 Power Supply tab fields

Field	Description
Desc	The power supply type.
OperStat	The operational state of the power supply. Possible values include: • other: Some other state. • notAvail: State not available. • removed: Component was removed. • disabled: Operation disabled. • normal: State is in normal operation. • resetInProg: There is a reset in progress. • testing: System is doing a self test. • warning: System is operating at a warning level. • nonFatalErr: System is operating at error level. • fatalErr: A fatal error stopped operation. • notConfig: A module needs to be configured. The allowable values are determined by the component type.

Fan tab

The Fan tab provides read-only information about the operating status of the switch fans.

To open the Fan tab:

1 From the menu bar, choose Edit > Chassis.

The Chassis dialog box opens (Figure 22) with the System tab displayed.

2 Click the Fan tab.

The Fan tab opens (Figure 30).

Figure 30 Edit Chassis dialog box — Fan tab

Table 25 describes the Fan tab fields.

Table 25 Fan tab fields

Field	Description
Desc	The fan type.
OperStat	The operational state of the fan. Values include: • other: Some other state. • notAvail: This state is not available. • removed: Fan was removed. • disabled: Fan is disabled. • normal: Fan is operating in normal operation. • resetInProg: A reset of the fan is in progress. • testing: Fan is doing a self test. • warning: Fan is operating at a warning level. • nonFatalErr: Fan is operating at error level. • fatalErr: An error stopped the fan operation • notConfig: Fan needs to be configured. The allowable values are determined by the component type.

CPU/Mem Utilization tab

The CPU/Mem Utilization tab provides read-only information about the utilization status of the switch CPU and memory.

To open the CPU/Mem Utilization tab:

1. Select the chassis.
2. From the shortcut menu, choose Edit > Chassis.

   The Chassis dialog box opens (Figure 22) with the System tab displayed.

3. Click the CPU/Mem Utilization tab.

   The CPU/Mem Utilization tab opens (Figure 31).

Figure 31 Edit Chassis dialog box — CPU/Mem Utilization tab

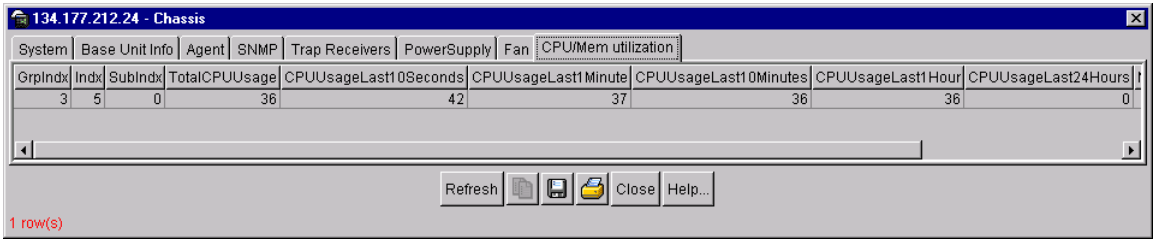


Table 25 describes the CPU/Mem Utilization tab fields.

Table 26 CPU/Mem Utilization tab fields

Field	Description
GrpIndx	The index of the chassis level group that contains this component. Corresponds to the s5ChasComGrpIndx MIB object.
Indx	The index of the component in the group. Corresponds to the s5ChasComIndx MIB object.
SubIndx	The sub-component index. Corresponds to the s5ChasComSubIndx MIB object.
TotalCPUUsage	The percentage of time the CPU has been busy over the last 1 minute.

Table 26 CPU/Mem Utilization tab fields (continued)

Field	Description
CPUUsageLast10Seconds	The percentage of time the CPU has been busy over the last 10 seconds.
CPUUsageLast1Minute	The percentage of time the CPU has been busy over the last 1 minute.
CPUUsageLast10Minutes	The percentage of time the CPU has been busy over the last 10 minutes.
CPUUsageLast1Hour	The percentage of time the CPU has been busy over the last 1 hour.
CPUUsageLast24Hours	The percentage of time the CPU has been busy over the last 24 hours.
MemoryAvailable	The percentage of dynamic memory that is currently free. The available memory is measured as a percentage of the memory that was available immediately after system initialization.
MemoryMinAvailable	The lowest percentage of dynamic memory that has been free since system initialization.

Working with configuration files

Use the FileSystem dialog box to view information and upload or download the configuration and image files.

Note: Do not use Device Manager to upgrade to Version 2.0 of the switch software. Instead, use either the command line interface (CLI), the console interface, or the Web-based management system. For more information, see *Using the Business Policy Switch 2000 Version 2.0*.

To open the Edit FileSystem dialog box:

➡ From the Device Manager main menu, choose Edit > File System.

The FileSystem dialog box opens (Figure 32).

Update only one item at a time. Click Apply after each change.

Figure 32 Edit FileSystem dialog box

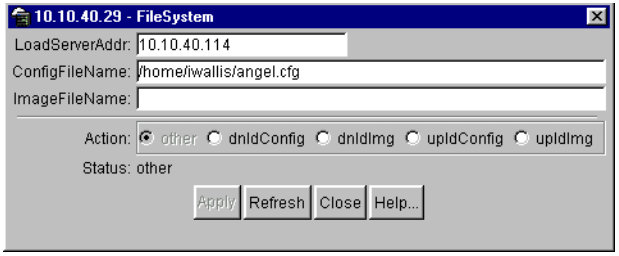


Table 27 describes the FileSystem dialog box items.

Table 27 FileSystem dialog box items

Item	Description
LoadServerAddr	The IP address of the load server for the configuration file and/or the image file. If not used, then the value is 0.0.0.0.
ConfigFileName	Name of the configuration file currently associated with the interface. When not used, the value is a zero length string.
ImageFileName	Name of the image file(s) currently associated with the interface. When the object is not used, the value is a zero length string.
450ImgFileName	Name of the image file(s) currently associated with any BayStack 450 units in the stack. When the object is not used, the value is a zero length string. This field is absent when there are no BayStack 450s in the stack.

Table 27 FileSystem dialog box items (continued)

Item	Description
Action	This object is used to download or upload a config file or an image file. In read operation, if there is no action taken since the boot up, it will return with a value of other. Otherwise, it will return the latest action such as: • dnldConfig • dnldImg • upldConfig In a write operation, the value that can be written is: • dnldConfig - download a config file to a device. The new config file will not take effect until the next boot cycle of the device. Possible values are: • dnldImg - download an image to a device. • upldConfig - upload a config file to a server from a device. The config file contains the current MIB object values of the device.
Status	This object is used to get the status of the latest action as shown by s5AgInfoFileAction. The values that can be read are: • other — if no action taken since the boot up • inProgress — the operation is in progress • success — the operation succeeds. • fail — the operation failed.

Graphing chassis statistics

To graph chassis statistics:

1. Select the chassis.
2. Do *one* of the following:
   - From the shortcut menu, choose Graph.
   - From Device Manager main menu, choose Graph > Chassis.
   - On the toolbar, click Graph.

The following sections describe the Graph Chassis dialog box tabs with descriptions of the statistics on each tab.

- "SNMP tab," next
- "IP tab" on page 78
- "ICMP In tab" on page 81
- "ICMP Out tab" on page 83

Six columns provide the statistics for the counters that are listed on the tab.

For descriptions of the chassis IP statistics, refer to Table 12 on page 44.

SNMP tab

The SNMP tab provides read-only information about the addresses that the agent software uses to identify the switch.For descriptions of the type of statistics shown in each column, refer to Table 28.

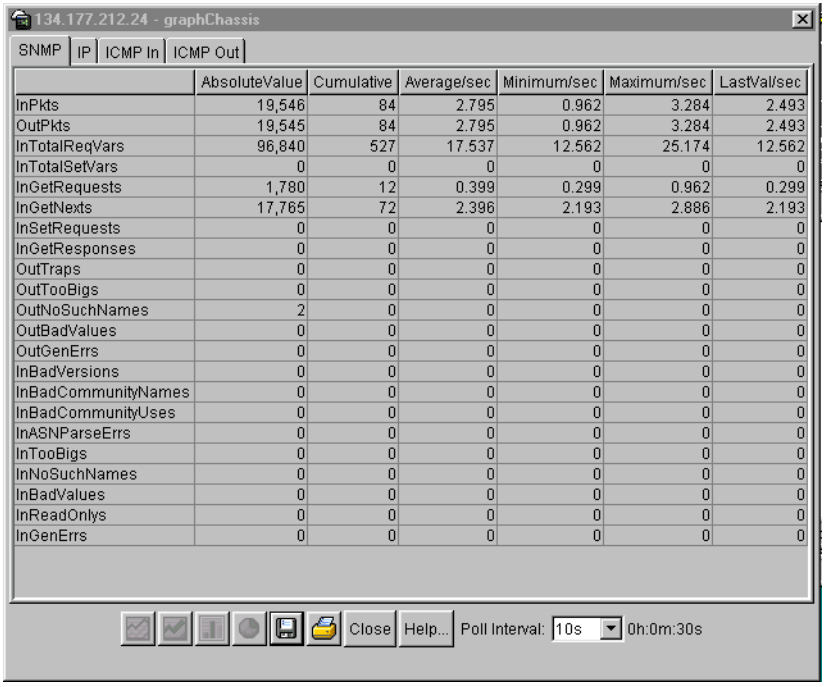
To open the SNMP tab:

1. Select the chassis.
2. From the shortcut menu, choose Graph > Chassis.

   The Chassis dialog box opens (Figure 22) with the System tab displayed.
3. Click the SNMP tab.

   The SNMP tab opens (Figure 33).

Figure 33 Graph Chassis dialog box — Chassis SNMP tab



	AbsoluteValue	Cumulative	Average/sec	Minimum/sec	Maximum/sec	LastVal/sec
InPkts	19,546	84	2.795	0.962	3.284	2.493
OutPkts	19,545	84	2.795	0.962	3.284	2.493
InTotalReqVars	96,840	527	17.537	12.562	25.174	12.562
InTotalSetVars	0	0	0	0	0	0
InGetRequests	1,780	12	0.399	0.299	0.962	0.299
InGetNexts	17,765	72	2.396	2.193	2.886	2.193
InSetRequests	0	0	0	0	0	0
InGetResponses	0	0	0	0	0	0
OutTraps	0	0	0	0	0	0
OutTooBigs	0	0	0	0	0	0
OutNoSuchNames	2	0	0	0	0	0
OutBadValues	0	0	0	0	0	0
OutGenErrs	0	0	0	0	0	0
InBadVersions	0	0	0	0	0	0
InBadCommunityNames	0	0	0	0	0	0
InBadCommunityUses	0	0	0	0	0	0
InASNParseErrs	0	0	0	0	0	0
InTooBigs	0	0	0	0	0	0
InNoSuchNames	0	0	0	0	0	0
InBadValues	0	0	0	0	0	0
InReadOnlys	0	0	0	0	0	0
InGenErrs	0	0	0	0	0	0

Table 28 describes the SNMP tab fields.

Table 28 SNMP tab fields

Field	Description
InPkts	The total number of messages delivered to the SNMP from the transport service.
OutPkts	The total number of SNMP messages passed from the SNMP protocol to the transport service.
InTotalReqVars	The total number of MIB objects retrieved successfully by the SNMP protocol as the result of receiving valid SNMP Get-Request and Get-Next PDUs.
InTotalSetVars	The total number of MIB objects altered successfully by the SNMP protocol as the result of receiving valid SNMP Set-Request PDUs.
InGetRequests	The total number of SNMP Get-Request PDUs that have been accepted and processed by the SNMP protocol.

Table 28 SNMP tab fields (continued)

Field	Description
InGetNexts	The total number of SNMP Get-Next PDUs accepted and processed by the SNMP protocol.
InSetRequests	The total number of SNMP Set-Request PDUs accepted and processed by the SNMP protocol.
InGetResponses	The total number of SNMP Get-Response PDUs accepted and processed by the SNMP protocol.
OutTraps	The total number of SNMP Trap PDUs generated by the SNMP protocol.
OutTooBigs	The total number of SNMP PDUs generated by the SNMP protocol for which the value of the error-status field is tooBig.
OutNoSuchNames	The total number of SNMP PDUs generated by the SNMP protocol for which the value of the error-status field is noSuchName.
OutBadValues	The total number of SNMP PDUs generated by the SNMP protocol for which the value of the error-status field is badValue.
OutGenErrs	The total number of SNMP PDUs generated by the SNMP protocol for which the value of the error-status field is genErr.
InBadVersions	The total number of SNMP messages delivered to the SNMP protocol for an unsupported SNMP version.
InBadCommunityNames	The total number of SNMP messages delivered to the SNMP protocol that used an unknown SNMP community name.
InBadCommunityUses	The total number of SNMP messages delivered to the SNMP protocol that represented an SNMP operation not allowed by the SNMP community named in the message.
InASNParseErrs	The total number of ASN.1 or BER errors encountered by the SNMP protocol when decoding received SNMP messages.
InTooBigs	The total number of SNMP PDUs delivered to the SNMP protocol for which the value of the error-status field is tooBig.
InNoSuchNames	The total number of SNMP PDUs delivered to the SNMP protocol for which the value of the error-status field is noSuchName.
InBadValues	The total number of SNMP PDUs delivered to the SNMP protocol for which the value of the error-status field is badValue.

Table 28 SNMP tab fields (continued)

Field	Description
InReadOnlys	The total number of SNMP PDUs delivered to the SNMP protocol for which the value of the error-status field is readOnly. It is a protocol error to generate an SNMP PDU containing the value “readOnly” in the error-status field. This object is provided to detect incorrect implementations of the SNMP.
InGenErrs	The total number of SNMP PDUs delivered to the SNMP protocol for which the value of the error-status field is genErr.

IP tab

The IP tab shows IP information for the chassis.

To open the IP tab:

1. Select the chassis.
2. Do *one* of the following:
   - From Device Manager main menu, choose Graph > Chassis.
   - From the shortcut menu, choose Graph.
   - On the toolbar, click Graph.

   The Chassis dialog box opens (Figure 33) with the SNMP tab displayed.
3. Click the IP tab.

   The IP tab opens (Figure 34).

Figure 34 Graph Chassis dialog box — IP tab

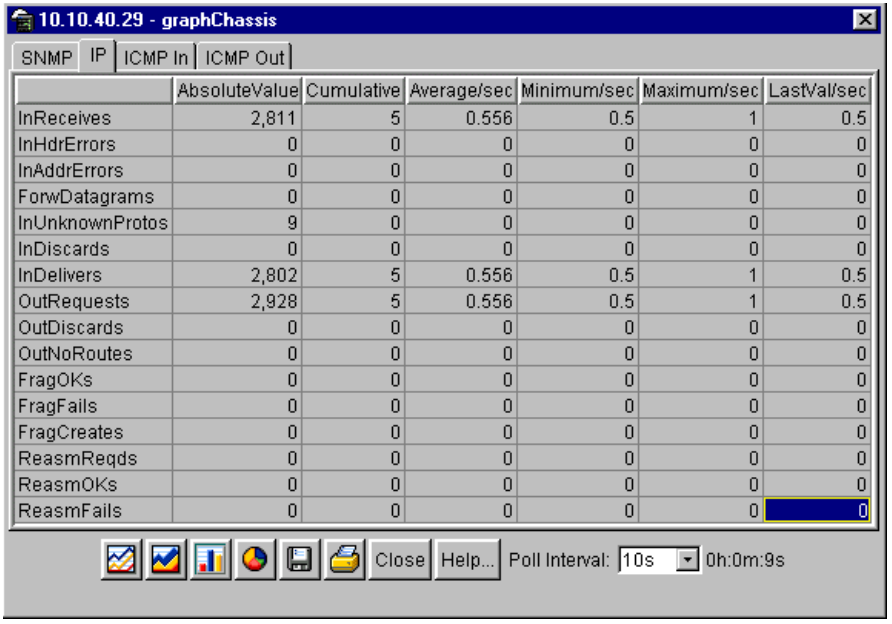

10.10.40.29 - graphChassis
SNMP
IP
ICMP In
ICMP Out
AbsoluteValue Cumulative Average/sec Minimum/sec Maximum/sec LastVal/sec
InReceives 2,811 5 0.556 0.5 1 0.5
InHdrErrors 0 0 0 0 0 0
InAddrErrors 0 0 0 0 0 0
ForwDatagrams 0 0 0 0 0 0
InUnknownProtos 9 0 0 0 0 0
InDiscards 0 0 0 0 0 0
InDelivers 2,802 5 0.556 0.5 1 0.5
OutRequests 2,928 5 0.556 0.5 1 0.5
OutDiscards 0 0 0 0 0 0
OutNoRoutes 0 0 0 0 0 0
FragOKs 0 0 0 0 0 0
FragFails 0 0 0 0 0 0
FragCreates 0 0 0 0 0 0
ReasmReqds 0 0 0 0 0 0
ReasmOKs 0 0 0 0 0 0
ReasmFails 0 0 0 0 0 0
Close
Help...
Poll Interval:
10s
0h:0m:9s

Table 29 describes the Chassis IP tab fields.

Table 29 Chassis IP tab fields

Field	Description
InReceives	The total number of input datagrams received from interfaces, including those received in error.
InHdrErrors	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options.
InAddrErrors	The number of input datagrams discarded because the IP address in the IP header destination field was not a valid address. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported Classes (for example, Class E). For addresses that are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.

Table 29 Chassis IP tab fields (continued)

Field	Description
ForwDatagrams	The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. For addresses that do not act as IP Gateways, this counter will include only those packets that were Source-Routed by way of this address and had successful Source-Route option processing.
InUnknownProtos	The number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
InDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing but that were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting reassembly.
InDelivers	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
OutRequests	The total number of IP datagrams that local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams.
OutDiscards	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but that were discarded (for example, for lack of buffer space). Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.
OutNoRoutes	The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams that meet this no-route criterion. Note that this includes any datagrams a host cannot route because all of its default gateways are down.
FragOKs	The number of IP datagrams that have been successfully fragmented at this entity.
FragFails	The number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be, for example, because their Don't Fragment flag was set.
FragCreates	The number of IP datagram fragments that have been generated as a result of fragmentation at this entity.
ReasmReqds	The number of IP fragments received that needed to be reassembled at this entity.

Table 29 Chassis IP tab fields (continued)

Field	Description
ReasmOKs	The number of IP datagrams successfully reassembled.
ReasmFails	The number of failures detected by the IP reassembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IP fragments because some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.

ICMP In tab

The chassis ICMP In tab shows ICMP In statistics.

To open the ICMP In tab:

1. Select the chassis.
2. Do *one* of the following:
   - From Device Manager main menu, choose Graph > Chassis.
   - From the shortcut menu, choose Graph.
   - On the toolbar, click Graph.

   The Chassis dialog box opens (Figure 33) with the SNMP tab displayed.
3. Click the ICMP In tab.

   The ICMP In tab opens (Figure 35).

Figure 35 Graph Chassis dialog box — ICMP In tab

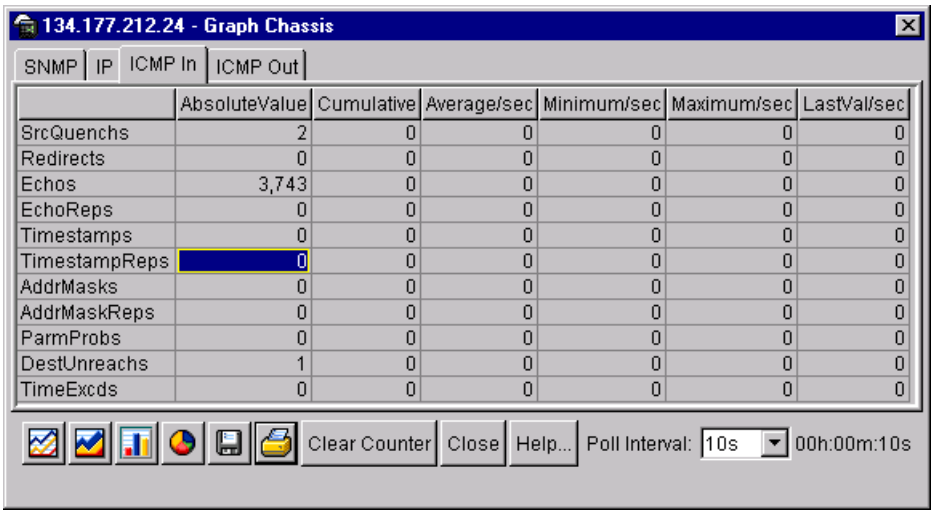


Table 30 describes the ICMP In tab fields.

Table 30 ICMP In tab fields

Field	Description
SrcQuenchs	The number of ICMP Source Quench messages received.
Redirects	The number of ICMP Redirect messages received.
Echos	The number of ICMP Echo (request) messages received.
EchoReps	The number of ICMP Echo Reply messages received.
Timestamps	The number of ICMP Timestamp (request) messages received.
TimestampReps	The number of ICMP Timestamp Reply messages received.
AddrMasks	The number of ICMP Address Mask Request messages received.
AddrMaskReps	The number of ICMP Address Mask Reply messages received.
ParmProbs	The number of ICMP Parameter Problem messages received.
DestUnreachs	The number of ICMP Destination Unreachable messages received.
TimeExcds	The number of ICMP Time Exceeded messages received.

ICMP Out tab

The chassis ICMP Out shows ICMP Out statistics.

To open the ICMP Out tab:

1 Select the chassis.

2 Do *one* of the following:

- From Device Manager main menu, choose Graph > Chassis.
- From the shortcut menu, choose Graph.
- On the toolbar, click Graph.

  The Chassis dialog box opens (Figure 33) with the SNMP tab displayed.

3 Click the ICMP Out tab.

  The ICMP Out tab opens (Figure 36).

Figure 36 Graph Chassis dialog box — ICMP Out tab

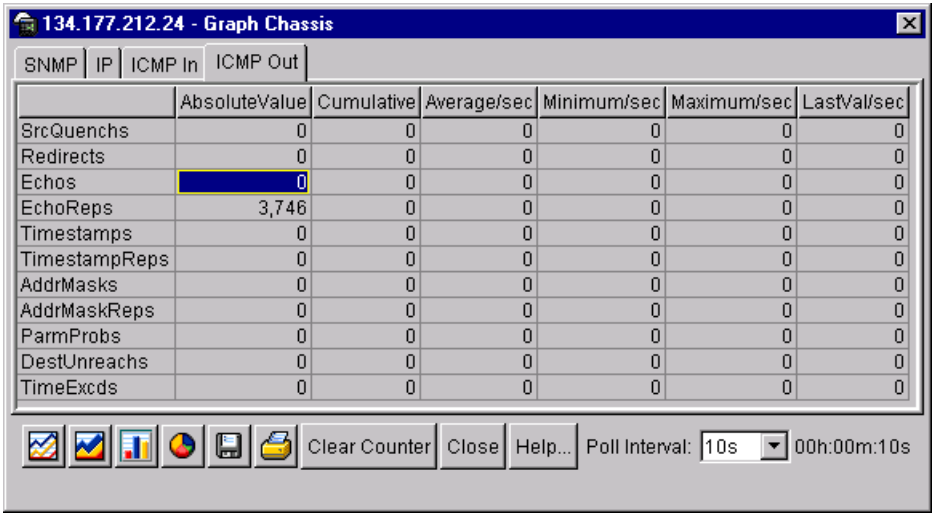


Table 31 describes the ICMP Out tab fields.

Table 31 ICMP Out tab fields

Field	Description
SrcQuenchs	The number of ICMP Source Quench messages sent.
Redirects	The number of ICMP Redirect messages received. For a host, this object will always be zero, because hosts do not send redirects.
Echos	The number of ICMP Echo (request) messages sent.
EchoReps	The number of ICMP Echo Reply messages sent.
Timestamps	The number of ICMP Timestamp (request) messages sent.
TimestampReps	The number of ICMP Timestamp Reply messages sent.
AddrMasks	The number of ICMP Address Mask Request messages sent.
AddrMaskReps	The number of ICMP Address Mask Reply messages sent.
ParmProbs	The number of ICMP Parameter Problem messages sent.
DestUnreachs	The number of ICMP Destination Unreachable messages sent.
TimeExcds	The number of ICMP Time Exceeded messages sent.

Chapter 3
Configuring and graphing ports

This chapter describes how you use Device Manager to configure and graph ports on a Business Policy Switch 2000.

The windows displayed when you configure a single port differ from the ones displayed when you configure multiple ports. However, the options are similar.

See the following sections for more information about configuring and graphing ports:

- "Viewing and editing a single port configuration," next
- "Viewing and editing multiple port configurations" on page 96
- "Graphing port statistics" on page 102

Viewing and editing a single port configuration

To view or edit the configuration of a single port, double-click on the port.

To view or edit the configuration of a single or multiple ports:

1. Select the port or ports you want to edit.
2. Do one of the following:
   - From the shortcut menu, choose Edit.
   - From the Device Manager main menu, choose Edit > Port.
   - Double-click on the selected port.
   - On the toolbar, click Edit.

Note: When you edit a single port, tabs that are not applicable are not available for you to select.

When you edit multiple ports, some tabs are not available, and some tabs are available even though the options are not applicable. When the option does not apply for a given port, NoSuchObject is displayed.

The following sections provide a description of the tabs in the Edit Port dialog box, and details about each field on the tab.

Interface tab for a single port

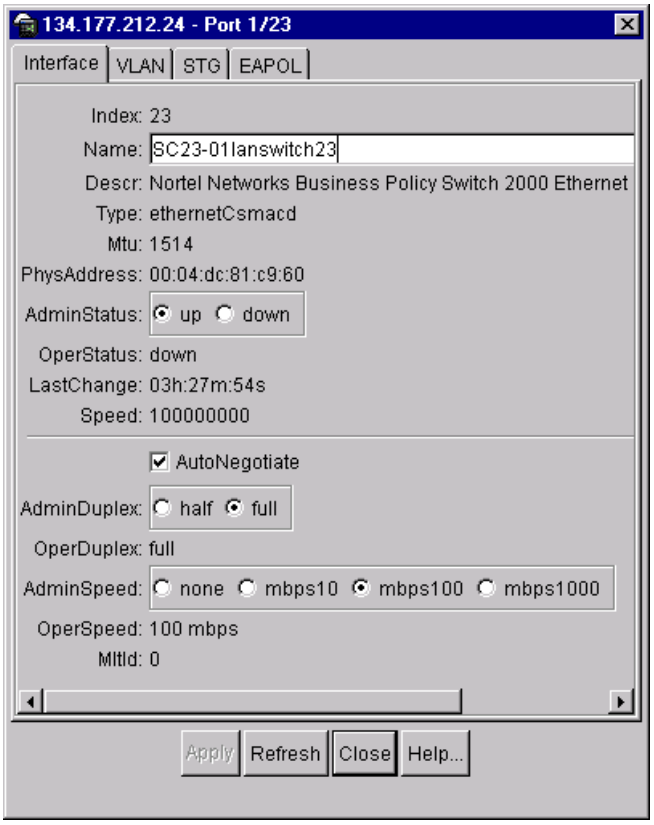
The Interface tab shows the basic configuration and status of a single port.

To view the Interface tab:

1. Select the port you want to edit.
2. Do one of the following:
   - Double-click on the selected port
   - From the shortcut menu, choose Edit.
   - From the Device Manager main menu, choose Edit > Port.
   - On the toolbar, click Edit button.

   The Port dialog box for a single port opens (Figure 37) with the Interface tab displayed.

Figure 37 Edit Port dialog box — Interface tab



Note: 10/100BASE-TX ports may not autonegotiate correctly with older 10/100BASE-TX equipment. In some cases, the older devices can be upgraded with new firmware or driver revisions. If an upgrade does not allow autonegotiation to correctly identify the link speed and duplex settings, you can manually configure the settings for the link in question. Check the Nortel Networks Web site (support.baynetworks.com/software) for the latest compatibility information.

Table 32 describes the Interface tab items for a single port.

Table 32 Interface tab items for a single port

Field	Description
Index	A unique value assigned to each interface. The value ranges between 12 and 255.
Name	Lets you enter a name for the port.
Descr	The type of switch and number of ports.
Type	The media type of this interface.
Mtu	The size of the largest packet, in octets, that can be sent or received on the interface.
PhysAddress	The MAC address assigned to a particular interface.
AdminStatus	The current administrative state of the interface, which can be one of the following: • up • down When a managed system is initialized, all interfaces start with AdminStatus in the down state. AdminStatus changes to the up state (or remains in the down state) as a result of either management action or the configuration information available to the managed system.

Table 32 Interface tab items for a single port (continued)

Field	Description
OperStatus	The current operational state of the interface, which can be one of the following: • up • down • testing If AdminStatus is up, then OperStatus should be up if the interface is ready to transmit and receive network traffic. If AdminStatus is down, then OperStatus should be down. It should remain in the down state if and only if there is a fault that prevents it from going to the up state. The testing state indicates that no operational packets can be passed.
LastChange	The value of sysUpTime at the time the interface entered its current operational state. If the current state was entered prior to the last reinitialization of the local network management subsystem, the value is zero.
Speed	The current speed of the port.
AutoNegotiate	Indicates whether this port is enabled for autonegotiation or not.
AdminDuplex	Sets the administrative duplex mode of the port (half or full).
OperDuplex	Shows the current administrative duplex mode of the port (half or full).
AdminSpeed	Set the port's speed.
OperSpeed	The current operating speed of the port.
MltId	The Multi-Link Trunk to which the port is assigned (if any).

VLAN tab for a single port

The VLAN tab allows you to view the VLAN membership for a single port.

To view the VLAN tab:

1. Select the port you want to edit.
2. Do one of the following:
   - Double-click the selected port
   - From the shortcut menu, choose Edit.
   - From the Device Manager main menu, choose Edit > Port.
   - On the toolbar, click Edit.

The Port dialog box for a single port opens (Figure 37) with the Interface tab displayed.

3 Click the VLAN tab.

The VLAN tab opens (Figure 38).

Figure 38 Edit Port dialog box — VLAN tab

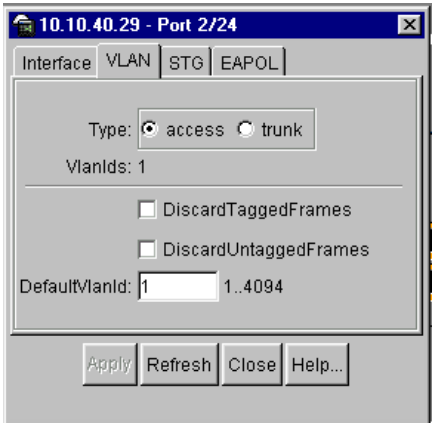


Table 33 describes the VLAN tab items.

Table 33 VLAN tab items for a single port

Item	Description
Type	Indicates the type of VLAN port (Trunk or Access port). If the port is a trunk port, the port is probably a member of more than one VLAN. If the port is an access port, the port can only be a member of one VLAN if there is no membership conflict.
VlanIds	The VLANIDs of which this port is a member.
DiscardTagged Frames	This field only applies to access ports. It acts as a flag used to determine how to process tagged frames received on this port. When the flag is set, the frames are discarded by the forwarding process. When the flag is reset, the frames are processed normally.

Table 33 VLAN tab items for a single port (continued)

Item	Description
DiscardUntaggedFrames	This field only applies to trunk ports. It acts as a flag used to determine how to process untagged frames received on this port. When the flag is set, the frames are discarded by the forwarding process. When the flag is reset, the frames are assigned to the VLAN specified by rcVlanPortDefaultVlanId.
DefaultVlanId	The VLAN ID assigned to untagged frames received on a trunk port.

STG tab for a single port

In the Spanning Tree Group (STG) tab, you can view the status and modify the configuration of a port's spanning tree parameters.

To view the STG tab:

1. Select the port you want to edit.
2. Do one of the following:
   - Double-click the selected port
   - From the shortcut menu, choose Edit.
   - From the Device Manager main menu, choose Edit > Port.
   - On the toolbar, click Edit.

   The Port dialog box for a single port opens (Figure 37) with the Interface tab displayed.
3. Click the STG tab.

   The STG tab opens (Figure 39).

Figure 39 Edit Port dialog box — STG tab

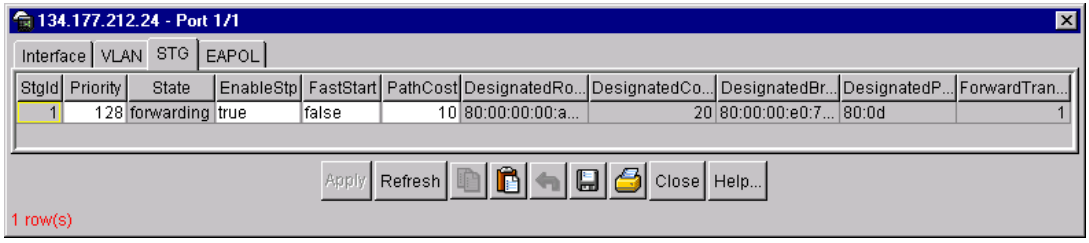


Table 34 describes the STG tab items.

Table 34 STG tab items for a single port

Item	Description
StgId	The number of times this port has transitioned from the Learning state to the Forwarding state.
Priority	The value of the priority field that is contained in the first (in network byte order) octet of the (2-octet long) Port ID. The other octet of the Port ID is derived from the value of dot1dStpPort.
State	The port's current state as defined by application of the Spanning Tree Protocol. This state controls the action a port takes when it receives a frame. If the bridge detects a port that is malfunctioning, it places that port into the broken state. For ports that are disabled (see EnableStp), this object has a value of disabled.
EnableStp	Allows you to select true or false to enable or disable STP.
FastStart	Allows you to select true or false to enable or disable FastStart.
PathCost	The contribution of this port to the cost of paths toward the spanning tree root, which include this port. The IEEE 802.1D-1990 standard recommends that the default value of this parameter be in inverse proportion to the speed of the attached LAN.
DesignatedRoot	The unique Bridge Identifier of the bridge recorded as the Root in the Configuration BPDUs transmitted by the Designated Bridge for the segment to which the port is attached.
DesignatedCost	The path cost of the Designated Port of the segment connected to this port. This value is compared to the Root Path Cost field in received bridge PDUs.
DesignatedBridge	The Bridge Identifier of the bridge that this port considers to be the Designated Bridge for this port's segment.
DesignatedPort	The Port Identifier of the port on the Designated Bridge for this port's segment.
ForwardTransitions	The number of times this port has transitioned from the Learning state to the Forwarding state.

EAPOL tab for a single port

The EAPOL tab allows you to configure EAPOL-based security for a single port.

To view the EAPOL tab:

1. Select the port you want to edit.
2. Do one of the following:
   - Double-click the selected port
   - From the shortcut menu, choose Edit.
   - From the Device Manager main menu, choose Edit > Port.
   - On the toolbar, click Edit.

   The Port dialog box for a single port opens (Figure 37) with the Interface tab displayed.
3. Click the EAPOL tab.

   The EAPOL tab opens (Figure 40).

Figure 40 Edit Port dialog box — EAPOL tab

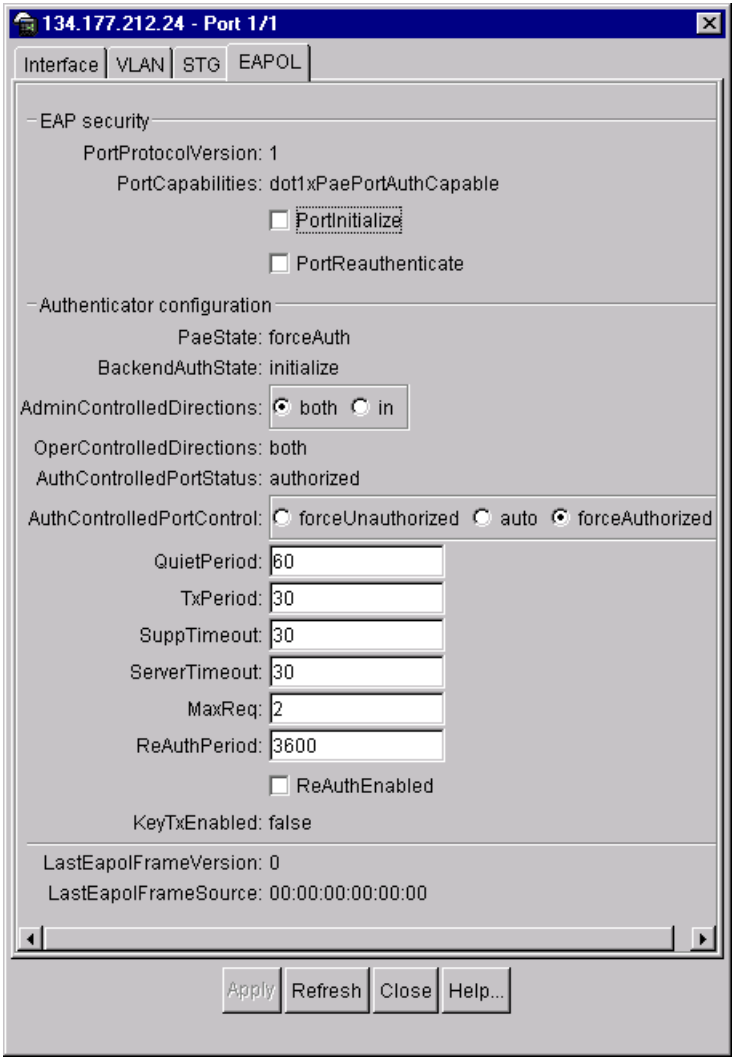


Table 35 describes the EAPOL tab items.

Table 35 EAPOL tab items for a single port

Item	Description
PortProtocolVersion	The EAP Protocol version that is running on this port.
PortCapabilities	The PAE functionality that is implemented on this port. Always returns dot1xPaePortAuthCapable(0).
PortInitialize	Setting this attribute to True causes this port's EAPOL state to be initialized.
PortReauthenticate	Setting this attribute to True causes the reauthentication of the client.
PaeState	The current authenticator PAE state machine stat value.
BackendAuthState	The current state of the Backend Authentication state machine.
AdminControlledDirections	The current value of the administrative controlled directions parameter for the port.
OperControlledDirections	The current value of the operational controlled directions parameter for the port.
AuthControlledPortStatus	The current value of the controlled port status parameter for the port.
AuthControlledPortControl	The current value of the controlled port control parameter for the port.
QuietPeriod	The current value of the time interval between authentication failure and the start of a new authentication.
TxPeriod	Time to wait for response from supplicant for EAP requests/ Identity packets.
SuppTimeout	Time to wait for response from supplicant for all EAP packets except EAP Request/Identity.
ServerTimeout	Time to wait for a response from the RADIUS server
MaxReq	Number of times to retry sending packets to the supplicant.
ReAuthPeriod	Time interval between successive re-authentications.
ReAuthEnabled	Whether to re-authenticate or not. Setting this object to Enabled causes reauthentication of existing supplicant at the time interval specified in the Re-authentication Period field.
KeyTxEnabled	The value of the KeyTranmissionEnabled constant currently in use by the Authenticator PAE state machine. This always returns false as key transmission is irrelevant.

Table 35 EAPOL tab items for a single port (continued)

Item	Description
LastEapolFrameVersion	The protocol version number carried in the most recently received EAPOL frame.
LastEapolFrameSource	The source MAC address carried in the most recently received EAPOL frame.

Viewing and editing multiple port configurations

To view or edit the configurations of multiple ports:

1 Select the ports you want to edit.

Press [Ctrl] + left click the ports you want to view or configure. A yellow outline appears around the selected ports.

2 Do one of the following:

- From the shortcut menu, choose Edit.
- From the Device Manager main menu, choose Edit > Port.
- Double-click on the selected port.
- On the toolbar, click Edit.

Note: When you edit multiple ports, some tabs are not available, and some tabs are available even though the options are not applicable. When the option does not apply for a given port, NoSuchObject is displayed.

Interface tab for multiple ports

The Interface tab shows the basic configuration and status of the selected ports.

To view or edit the Interface tab for multiple ports:

1 Select the ports that you want to edit.

[Ctrl] + left-click the ports that you want to configure. A yellow outline appears around the selected ports.

2 Do one of the following:

- From the shortcut menu, choose Edit.
- From the Device Manager main menu, choose Edit > Port.
- On the toolbar, click Edit.

The Port dialog box for multiple ports opens with the Interface tab (Figure 41) displayed.

Figure 41 Port dialog box — Port Interface tab

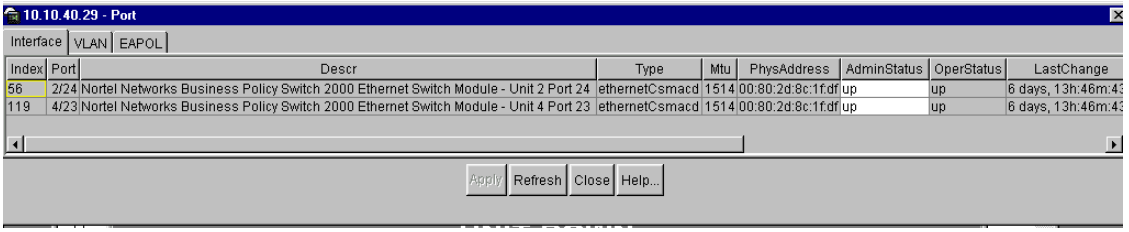


Table 36 describes the Port Interface tab fields.

Table 36 Interface tab fields for multiple ports

Field	Description
Index	A unique value assigned to each interface. The value ranges between 12 and 255.
Descr	Type of switch and number of ports.
Type	Media type for this interface.
Mtu	Size of the largest packet, in octets, that can be sent or received on the interface.
PhysAddress	MAC address assigned to a particular interface.

Table 36 Interface tab fields for multiple ports (continued)

Field	Description
AdminStatus	Current administrative state of the interface, which can be one of the following: • up • down When a managed system is initialized, all interfaces start with AdminStatus in the down state. AdminStatus changes to the up state (or remains in the down state) as a result of either management action or the configuration information available to the managed system.
OperStatus	Current operational state of the interface, which can be one of the following: • up • down • testing If AdminStatus is up, then OperStatus should be up if the interface is ready to transmit and receive network traffic. If AdminStatus is down, then OperStatus should be down. It should remain in the down state if and only if there is a fault that prevents it from going to the up state. The testing state indicates that no operational packets can be passed.
LastChange	Value of the time the interface entered its current operational state. If the current state was entered prior to the last reinitialization of the local network management subsystem, the value is zero.
Speed	The estimate bandwidth of the interface in bits per second (bps). For interfaces that do not vary in bandwidth or have no way to estimate the bandwidth, this object should contain the nominal bandwidth. If the bandwidth of the interface is greater than the maximum value reported by the object, then the object displays its maximum value (4,294,967,295). For a sub-layer that has no concept of bandwidth, the object should be zero.
AutoNegotiate	Indicates whether the port is enabled (checked) for autonegotiation or not.
AdminDuplex	The current administrative duplex mode of the port (half or full).
OperDuplex	Indicate current duplex value of the port.
AdminSpeed	Set the speed of a port: none, mbps10, and mbps100
OperSpeed	The current operating speed of the port.
MltId	The MultiLink Trunk to which the port is assigned (if any).

VLAN tab for multiple ports

The VLAN tab shows the VLAN membership for the selected ports.

To view or edit the VLAN tab for multiple ports:

1 Select the ports that you want to edit.

[Ctrl] + left-click the ports that you want to configure. A yellow outline appears around the selected ports.

2 Do one of the following:

- From the shortcut menu, choose Edit.
- From the Device Manager main menu, choose Edit > Port.
- On the toolbar, click Edit.

The Port dialog box for a multiple port (Figure 37) opens with the Interface tab displayed.

3 Click the VLAN tab.

The VLAN tab opens (Figure 42).

Figure 42 VLAN tab for multiple ports

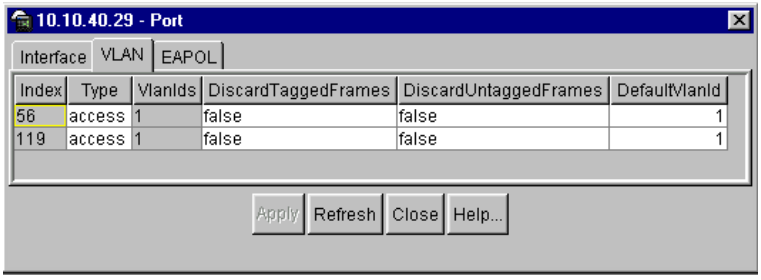


Table 37 describes the VLAN tab fields for multiple ports.

Table 37 VLAN tab fields for multiple ports

Field	Description
Type	Indicates the type of VLAN port (Trunk or Access port). If the port is a trunk port, the port is probably a member of more than one VLAN. If the port is an access port, the port can only be a member of one VLAN if there is no membership conflict.
VlanIds	The VLANIDs of which this port is a member.
DiscardTaggedFrames	This field only applies to access ports. It acts as a flag used to determine how to process tagged frames received on this port. When the flag is set, the frames are discarded by the forwarding process. When the flag is reset, the frames are processed normally.
DiscardUntaggedFrames	This field only applies to trunk ports. It acts as a flag used to determine how to process untagged frames received on this port. When the flag is set, the frames are discarded by the forwarding process. When the flag is reset, the frames are assigned to the VLAN specified by rcVlanPortDefaultVlanId.
DefaultVlanId	The VLAN ID assigned to untagged frames received on a trunk port.

EAPOL tab for multiple ports

The EAPOL tab shows EAPOL statistics for the selected ports.

To view or edit the EAPOL tab for multiple ports:

1 Select the ports that you want to edit.

[Ctrl] + left-click the ports that you want to configure. A yellow outline appears around the selected ports.

2 Do one of the following:

- From the shortcut menu, choose Edit.
- From the Device Manager main menu, choose Edit > Port.
- On the toolbar, click Edit.

The Port dialog box for a multiple port (Figure 37) opens with the Interface tab displayed.

3 Click the EAPOL tab.

The EAPOL tab opens (Figure 43).

Figure 43 EAPOL tab for multiple ports

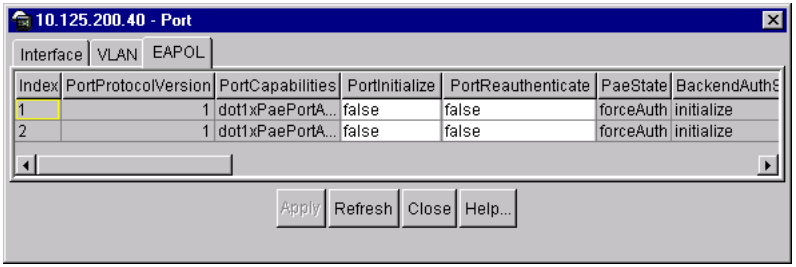


Table 38 describes the EAPOL tab fields for multiple ports.

Table 38 EAPOL tab fields for multiple ports

Field	Description
Index	Displays the unique value assigned to each interface.
PortProtocolVersion	The EAP Protocol version that is running on this port.
PortCapabilities	The PAE functionality that is implemented on this port. Always returns dot1xPaePortAuthCapable(0).
PortInitialize	Setting this attribute to True causes this port's EAPOL state to be initialized.
PortReauthenticate	Setting this attribute to True causes the reauthentication of the client.
PaeState	The current authenticator PAE state machine stat value.
BackendAuthState	The current state of the Backend Authentication state machine.
AdminControlledDirections	The current value of the administrative controlled directions parameter for the port.
OperControlledDirections	The current value of the operational controlled directions parameter for the port.
AuthControlledPortStatus	The current value of the controlled port status parameter for the port.
AuthControlledPortControl	The current value of the controlled port control parameter for the port.

Table 38 EAPOL tab fields for multiple ports (continued)

Field	Description
QuietPeriod	The current value of the time interval between authentication failure and the start of a new authentication.
TxPeriod	Time to wait for response from supplicant for EAP requests/Identity packets.
SuppTiemout	Time to wait for response from supplicant for all EAP packets except EAP Request/Identity.
ServerTimeout	Time to wait for a response from the RADIUS server
MaxReq	Number of times to retry sending packets to the supplicant.
ReAuthPeriod	Time interval between successive re-authentications.
ReAuthEnabled	Whether to re-authenticate or not. Setting this object to Enabled causes reauthentication of existing supplicant at the time interval specified in the Re-authentication Period field.
KeyTxEnabled	The value of the KeyTranmissionEnabled constant currently in use by the Authenticator PAE state machine. This always returns false as key transmission is irrelevant.
LastEapolFrameVersion	The protocol version number carried in the most recently received EAPOL frame.
LastEapolFrameSource	The source MAC address carried in the most recently received EAPOL frame.

Graphing port statistics

You can graph statistics for either a single port or multiple ports from the graphPort dialog box. The windows displayed are identical for either single or multiple port configuration.

To open the graphPort dialog box for graphing:

1 Select the port or ports you want to graph.

To select multiple ports, [Ctrl] + left-click the ports that you want to configure. A yellow outline appears around the selected ports.

2 Do one of the following:

- From the Device Manager main menu, choose Graph > Port.
- From the shortcut menu, choose Graph.
- On the toolbar, click Graph.

The graphPort dialog box for a single port or for multiple ports opens with the Interface tab displayed.

Note: Some statistics are only available when you graph a single port.

Interface tab for graphing ports

The Interface tab shows interface parameters for graphing a port or ports.

To open the Interface tab for graphing:

1 Select the port or ports you want to graph.

To select multiple ports, [Ctrl] + left-click the ports that you want to configure. A yellow outline appears around the selected ports.

2 Do one of the following:

- From the Device Manager main menu, choose Graph > Port.
- From the shortcut menu, choose Graph.
- On the toolbar, click Graph.

The Port dialog box for a single port or for multiple ports (Figure 44) opens with the Interface tab displayed.

Figure 44 Interface tab for graphing ports

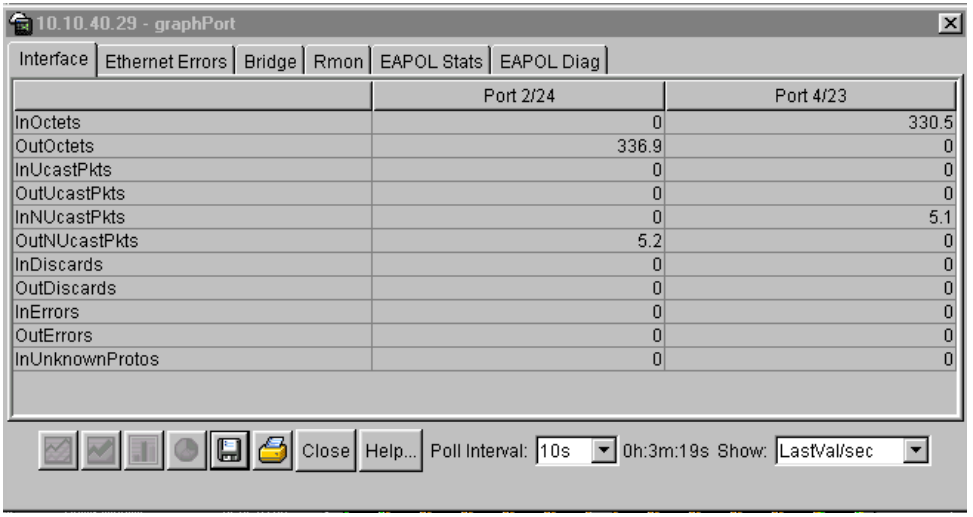


Table 39 describes the Interface tab fields for graphing ports.

Table 39 Port Interface tab fields for multiple ports

Field	Description
ifInOctets	The total number of octets received on the interface, including framing characters.
ifOutOctets	The total number of octets transmitted out of the interface, including framing characters.
ifInUcastPkts	The number of packets delivered by this sublayer to a higher sublayer that were not addressed to a multicast or broadcast address at this sublayer.
ifOutUcastPkts	The number of packets that higher-level protocols requested be transmitted that were not addressed to a multicast address at this sublayer. This total number includes those packets discarded or unsent.
ifInNUcastPkts	The number of packets delivered by this sublayer to a higher (sub)layer, which were addressed to a multicast or broadcast address at this sublayer.
ifOutNUcastPkts	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast or broadcast address at this sublayer, including those that were discarded or not sent.

Table 39 Port Interface tab fields for multiple ports (continued)

Field	Description
InDiscards	The number of inbound packets that were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
OutDiscards	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
InErrors	For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol.
OutErrors	For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors.
InUnknownProtos	For packet-oriented interfaces, the number of packets received via the interface that were discarded because of an unknown or unsupported protocol. For character-oriented or fixed-length interfaces that support protocol multiplexing, the number of transmission units received via the interface that were discarded because of an unknown or unsupported protocol. For any interface that does not support protocol multiplexing, this counter will always be 0.

Ethernet Errors tab for graphing ports

The port Ethernet Errors tab shows port Ethernet Errors statistics.

To open the Ethernet Errors tab for graphing:

1 Select the port or ports you want to graph.

To select multiple ports, [Ctrl] + left-click the ports that you want to configure. A yellow outline appears around the selected ports.

2 Do one of the following:

- From the Device Manager main menu, choose Graph > Port.

- From the shortcut menu, choose Graph.
- On the toolbar, click Graph.

The Port dialog box for a single port or for multiple ports opens with the Interface tab displayed.

3 Click the Ethernet Errors tab.

The Port Ethernet Errors tab (Figure 45) opens.

Figure 45 Graph Port dialog box — Port Ethernet Errors tab

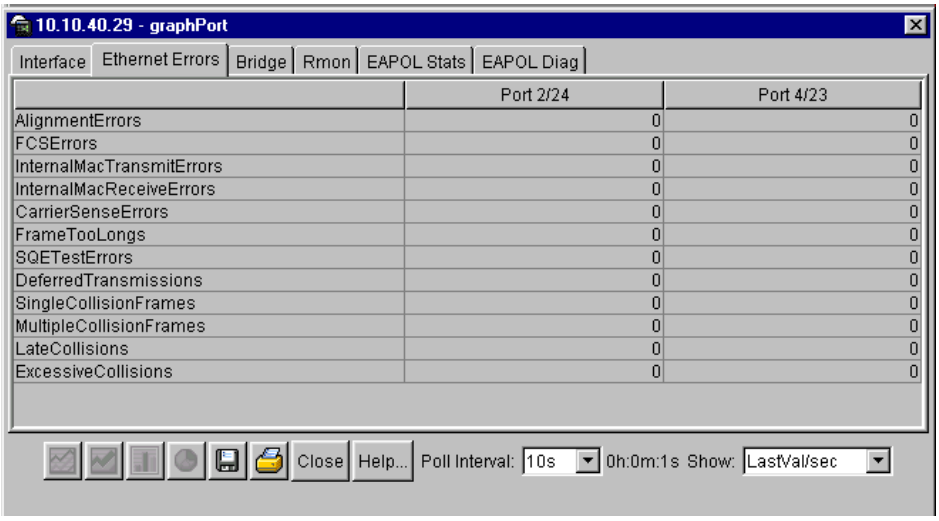


Table 40 describes the Port Ethernet Errors tab fields.

Table 40 Ethernet Errors tab fields

Field	Description
AlignmentErrors	A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check. The count represented by an instance of this object is incremented when the alignmentError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
FCSErrors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. The count represented by an instance of this object is incremented when the frameCheckError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
InternalMacTransmitErrors	A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the LateCollisions object, the ExcessiveCollisions object, or the CarrierSenseErrors object.
InternalMacReceiveErrors	A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the FrameTooLongs object, the AlignmentErrors object, or the FCSErrors object. The precise meaning of the count represented by an instance of this object is implementation specific. In particular, an instance of this object may represent a count of receive errors on a particular interface that are not otherwise counted.
CarrierSenseErrors	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular interface. The count represented by an instance of this object is incremented at most once per transmission attempt, even if the carrier sense condition fluctuates during a transmission attempt.

Table 40 Ethernet Errors tab fields (continued)

Field	Description
FrameTooLongs	A count of frames received on a particular interface that exceed the maximum permitted frame size. The count represented by an instance of this object is incremented when the frameTooLong status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
SQETestErrors	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface. The SQE TEST ERROR message is defined in section 7.2.2.2.4 of ANSI/IEEE 802.3-1985 and its generation is described in section 7.2.4.6 of the same document.
DeferredTransmissions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy. The count represented by an instance of this object does not include frames involved in collisions.
SingleCollisionFrames	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the MultipleCollisionFrames object.
MultipleCollisionFrames	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the SingleCollisionFrames object.
LateCollisions	The number of times that a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet. Five hundred and twelve bit-times corresponds to 51.2 microseconds on a 10 Mb/s system. A (late) collision included in a count represented by an instance of this object is also considered as a (generic) collision for purposes of other collision-related statistics.
ExcessiveCollisions	A count of frames for which transmission on a particular interface fails due to excessive collisions.
Poll Interval	Statistics are updated based on the poll interval.

Table 40 Ethernet Errors tab fields (continued)

Field	Description
	Default: 10s
	Range: None, 2s, 5s, 10s, 30s, 1m, 5m, 30m 1h

Bridge tab for graphing ports

The Bridge tab displays port frame statistics.

To open the Bridge tab for graphing:

1. Select the port or ports you want to graph.

   To select multiple ports, [Ctrl] + left-click the ports that you want to configure. A yellow outline appears around the selected ports.

2. Do one of the following:

   - From the Device Manager main menu, choose Graph > Port.
   - From the shortcut menu, choose Graph.
   - On the toolbar, click Graph.

   The Port dialog box for a single port or for multiple ports opens with the Interface tab displayed.

3. Click the Bridge tab.

   The Bridge tab for graphing ports opens (Figure 46).

Figure 46 Graph Port dialog box — Bridge tab

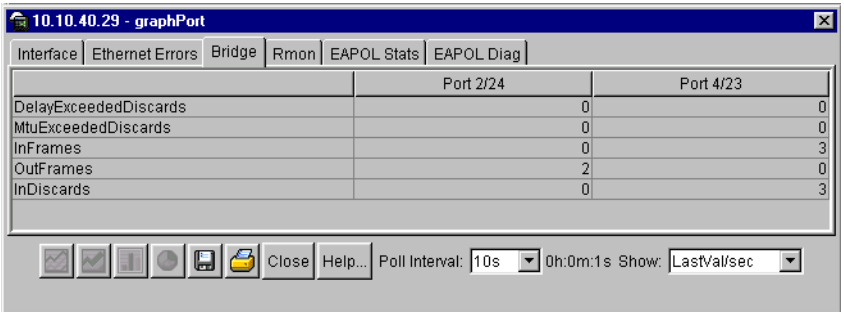


Table 41 describes the Bridge tab fields.

Table 41 Bridge tab fields

Field	Description
DelayExceededDiscards	Number of frames discarded by the port due to excessive transit delays through the bridge. It is incremented by both transparent and source route bridges.
MtuExceededDiscards	Number of frames discarded by the port due to an excessive size. It is incremented by both transparent and source route bridges.
InFrames	The number of frames that have been received by this port from its segment.
OutFrames	The number of frames that have been received by this port from its segment.
InDiscards	Count of valid frames received which were discarded (filtered) by the Forwarding Process.

RMON tab for graphing ports

The RMON tab displays Ethernet statistics for graphing a port or ports.

To open the RMON tab for graphing:

1 Select the port or ports you want to graph.

To select multiple ports, [Ctrl] + left-click the ports that you want to configure. A yellow outline appears around the selected ports.

2 Do one of the following:

- From the Device Manager main menu, choose Graph > Port.
- From the shortcut menu, choose Graph.
- On the toolbar, click Graph.

The Port dialog box for a single port or for multiple ports opens with the Interface tab displayed.

3 Click the RMON tab.

The RMON tab for graphing multiple ports opens (Figure 47).

Figure 47 Graph Port dialog box — RMON tab

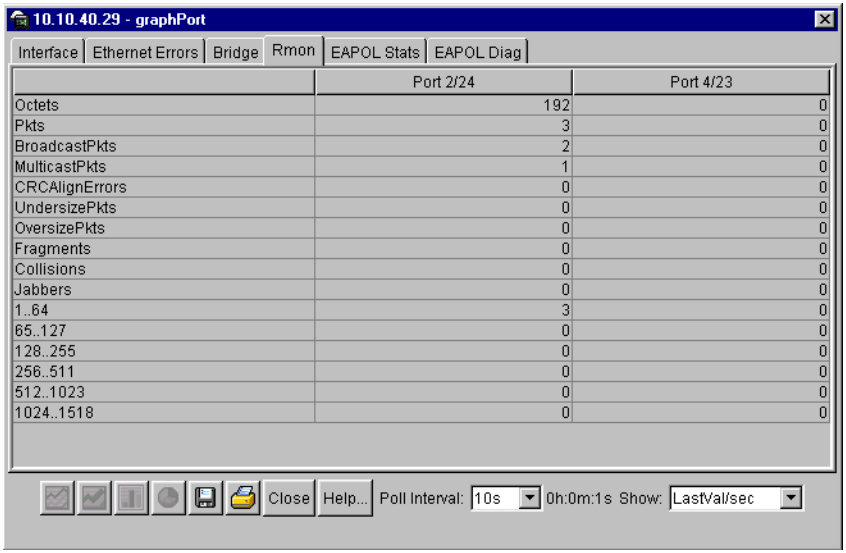


Table 42 describes the RMON tab fields.

Table 42 RMON tab fields

Field	Description
Octets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). You can use this object as a reasonable estimate of Ethernet utilization. For greater precision, sample the etherStatsPkts and etherStatsOctets objects before and after a common interval.
Pkts	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
BroadcastPkts	The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.
MulticastPkts	The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
CRCAlignErrors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error).

Table 42 RMON tab fields (continued)

Field	Description
UndersizePkts	The total number of packets received that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.
OversizePkts	The total number of packets received that were longer than 1518 octets (excluding framing bits but including FCS octets) and were otherwise well formed.
Fragments	The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error). It is entirely normal for etherStatsFragments to increment because it counts both runts (which are normal occurrences due to collisions) and noise hits.
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
Jabbers	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Jabber is defined as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.
1..64	The total number of packets (including bad packets) received that were between 1 and 64 octets in length (excluding framing bits but including FCS octets).
65..127	The total number of packets (including bad packets) received that were between 65 and 127 octets in length (excluding framing bits but including FCS octets).
128..255	The total number of packets (including bad packets) received that were between 128 and 255 octets in length (excluding framing bits but including FCS octets).
256..511	The total number of packets (including bad packets) received that were between 256 and 511 octets in length (excluding framing bits but including FCS octets).
511..1023	The total number of packets (including bad packets) received that were between 511 and 1023 octets in length (excluding framing bits but including FCS octets).
1024..1518	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length (excluding framing bits but including FCS octets).

EAPOL Stats tab for graphing ports

The EAPOL Stats tab displays EAPOL statistics.

To open the EAPOL Stats tab for graphing:

1 Select the port or ports you want to graph.

To select multiple ports, [Ctrl] + left-click the ports that you want to configure. A yellow outline appears around the selected ports.

2 Do one of the following:

- From the Device Manager main menu, choose Graph > Port.
- From the shortcut menu, choose Graph.
- On the toolbar, click Graph.

The Port dialog box for a single port or for multiple ports opens with the Interface tab displayed.

3 Click the EAPOL Stats tab.

The EAPOL Stats tab for graphing multiple ports opens (Figure 48).

Figure 48 Graph Port dialog box — EAPOL Stats tab

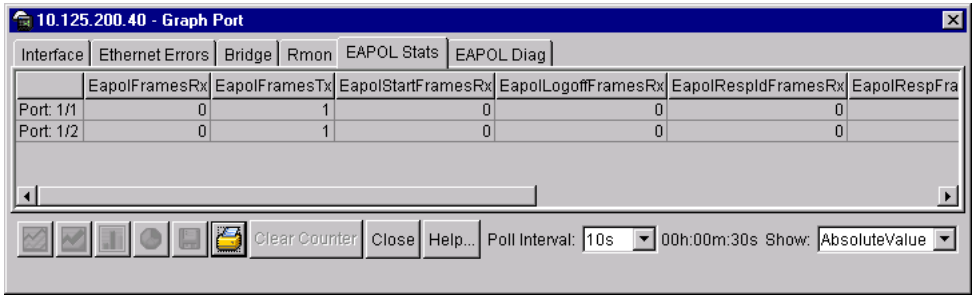


Table 43 describes the EAPOL tab fields.

Table 43 EAPOL tab fields

Field	Description
EapolFramesRx	The number of valid EAPOL frames of any type that have been received by this authenticator.
EapolFramesTx	The number of EAPOL frame types of any type that have been transmitted by this authenticator.
EapolStartFramesRx	The number of EAPOL start frames that have been received by this authenticator.
EapolLogoffFramesRx	The number of EAPOL Logoff frames that have been received by this authenticator.
EapolRespIdFramesRx	The number of EAPOL Resp/Id frames that have been received by this authenticator.
EapolRespFramesRx	The number of valid EAP Response frames (Other than Resp/Id frames) that have been received by this authenticator.
EapolReqIdFramesTx	The number of EAPOL Req/Id frames that have been transmitted by this authenticator.
EapolReqFramesTx	The number of EAP Req/Id frames (Other than Rq/Id frames) that have been transmitted by this authenticator.
InvalidEapolFramesRx	The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.
EapLengthErrorFramesRx	The number of EAPOL frames that have been received by this authenticator in which the packet body length field is not valid.

EAPOL Diag tab for graphing ports

The EAPOL Diag tab displays EAPOL diagnostics statistics.

To open the EAPOL Diag tab for graphing:

1 Select the port or ports you want to graph.

To select multiple ports, [Ctrl] + left-click the ports that you want to configure. A yellow outline appears around the selected ports.

2 Do one of the following:

- From the Device Manager main menu, choose Graph > Port.
- From the shortcut menu, choose Graph.
- On the toolbar, click Graph.

The Port dialog box for a single port or for multiple ports opens with the Interface tab displayed.

3 Click the EAPOL Diag tab.

The EAPOL Diag tab for graphing multiple ports opens (Figure 49).

Figure 49 Graph Port dialog box — EAPOL Diag tab

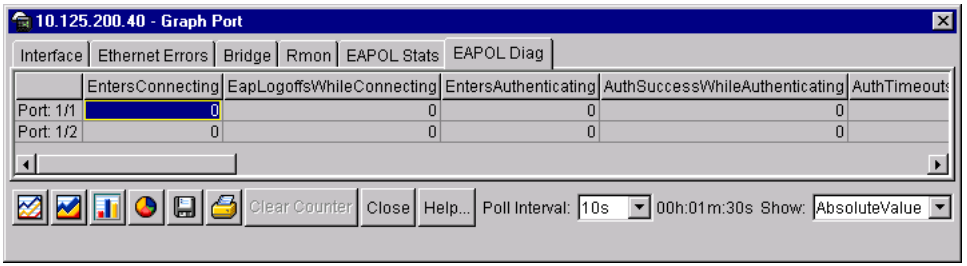


Table 44 describes the EAPOL Diag tab fields.

Table 44 EAPOL Diag tab fields

Field	Description
EntersConnecting	Counts the number of times that the Authenticator PAE state machine transitions to the Connecting state from any other state.
EapLogoffsWhileConnecting	Counts the number of times that the Authenticator PAE state machine transitions from Connected to Disconnected as a result of receiving an EAPOL-Logoff message.
EntersAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Connecting to Authenticating as a result of receiving an EAP-Response/Identity message being received from the supplicant.
AuthSuccessWhileAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Authenticated as a result of the Backend authentication state machine indicating successful authentication of the supplicant.
AuthTimeoutsWhile Authenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Aborting as a result of the Backend authentication state machine indicating authentication timeout.
AuthFailWhileAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Held as a result of the Backend authentication state machine indicating authentication failure.
AuthReauthsWhileAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Aborting as a result of a reauthentication request.
AuthEapStartsWhileAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Aborting as a result of an EAPOL-Start message being received from the supplicant.
AuthEapLogoffWhileAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Aborting as a result of an EAPOL-Logoff message being received from the supplicant.
AuthReauthsWhileAuthenticated	Counts the number of times that the Authenticator PAE state machine transitions from Authenticated to Connecting as a result of a reauthentication request.

Table 44 EAPOL Diag tab fields (continued)

Field	Description
AuthEapStartsWhileAuthenticated	Counts the number of times that the Authenticator PAE state machine transitions from Authenticated to Connecting as a result of an EAPOL-Start message being received from the supplicant.
AuthEapLogoffWhileAuthenticated	Counts the number of times that the Authenticator PAE state machine transitions from Authenticated to Disconnected as a result of an EAPOL-Logoff message being received from the supplicant.
BackendResponses	Counts the number of times that the Backend Authentication state machine sends an Initial-Access request packet to the Authentication server.
BackendAccessChallenges	Counts the number of times that the Backend Authentication state machine receives an Initial-Access challenge packet from the Authentication server.
BackendOtherRequestsToSupplicant	Counts the number of times that the Backend Authentication state machine sends an EAP request packet (other than an Identity, Notification, failure, or success message) to the supplicant.
BackendNonNakResponsesFromSupplicant	Counts the number of times that the Backend Authentication state machine receives a response from the supplicant to an initial EAP request and the response is something other than EAP-NAK.
BackendAuthSuccesses	Counts the number of times that the Backend Authentication state machine receives an EAP-success message from the Authentication server.
BackendAuthFails	Counts the number of times that the Backend Authentication state machine receives an EAP-failure message from the Authentication server.

Chapter 4
Setting up MultiLink Trunk ports

MultiLink Trunking (MLT) is a point-to-point connection that aggregates multiple ports so that they logically act like a single port with the aggregated bandwidth. Grouping multiple ports into a logical link allows you to achieve higher aggregate throughput on a switch-to-switch or switch-to-server application. MultiLink Trunking provides media and module redundancy.

MultiLink Trunk (MLT) features

A number of Nortel Networks products implement MultiLink Trunking and have different features and requirements based on the architecture of the device. For the Business Policy Switch, MultiLink Trunking has the following general features and requirements:

- A unit can have up to six MultiLink Trunks (MLTs).
- Up to four ports can belong to an MLT.
- The ports in an MLT can be on different unit in the stack.
- MultiLink Trunking is supported on 10BASE-T, 100BASE-TX, 100BASE-FX, and Gigabit Ethernet ports.
- MultiLink Trunking is compatible with the Spanning Tree Protocol.
- IEEE 802.1Q tagging is supported on an MLT.
- For bridge traffic, the algorithm that distributes traffic across an MLT is based on the source and destination MAC addresses.

Setting up MLTs

To set up MLTs:

➨ From the Device Manager menu bar, choose VLAN > MLT.

The MLT dialog box opens (Figure 50).

Figure 50 MLT dialog box

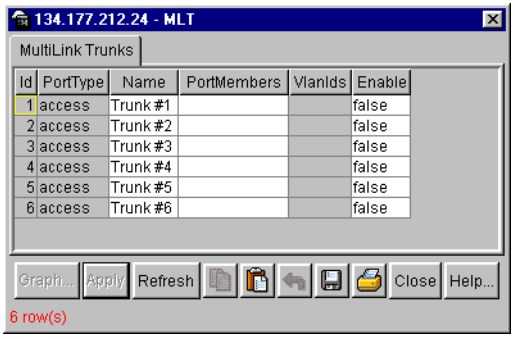

134.177.212.24 - MLT
MultiLink Trunks
Id PortType Name PortMembers VlanIds Enable
1 access Trunk #1 false
2 access Trunk #2 false
3 access Trunk #3 false
4 access Trunk #4 false
5 access Trunk #5 false
6 access Trunk #6 false
Graph... Apply Refresh Close Help...
6 row(s)

Table 45 describes the fields of the MLT dialog box.

Table 45 MLT dialog box fields

Field	Description
ID	The number of the MLT (assigned consecutively).
Name	The name given to the MLT.
PortType	Access or trunk port.
PortMembers	The ports that are assigned to the MLT.
VlanIds	Specifies the VLAN identifier.
Enable	Specifies whether the multilink trunk is active or not.

Adding ports to a MultiLink Trunk

To add ports to an existing MLT:

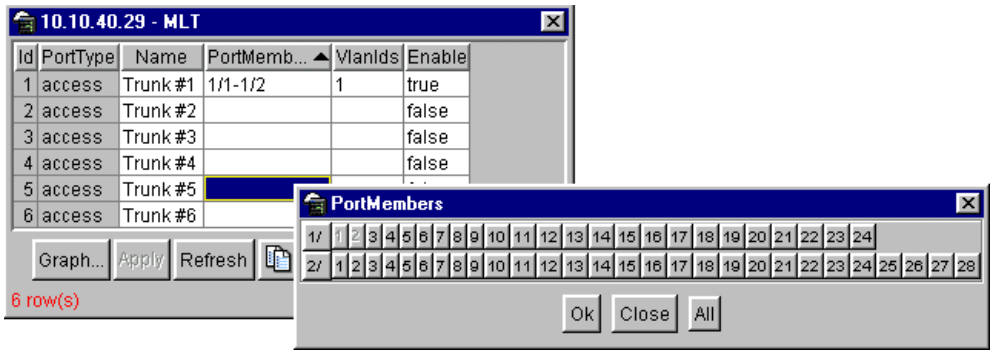
1 From the Device Manager menu bar, choose VLAN > MLT.

The MLT dialog box opens.

2 Double-click the PortMembers field.

The PortMembers dialog box opens (Figure 51).

Figure 51 PortMembers dialog box


10.10.40.29 - MLT
Id
PortType
Name
PortMemb...
VlanIds
Enable
1 access Trunk #1 1/1-1/2 1 true
2 access Trunk #2 false
3 access Trunk #3 false
4 access Trunk #4 false
5 access Trunk #5
6 access Trunk #6
Graph...
Apply
Refresh
6 row(s)
PortMembers
1/ 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
2/ 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28
Ok
Close
All

3 Click the port numbers you want to add.

4 Click OK.

5 In the Enable column, select True to enable your selection.

Note: The first enabled distributed MLT causes the stack to reset. Please refer to the switch manuals for more details on MLT rules.

MultiLink Trunk statistics

To view MLT interface statistics:

1 From the Device Manager menu bar, choose VLAN > MLT.

The MLT window opens (Figure 52).

2 Select an MLT row and then click Graph.

The Statistics, MLT window (Figure 52) opens with the Interface tab displayed.

Figure 52 MLT Statistics — Interface tab

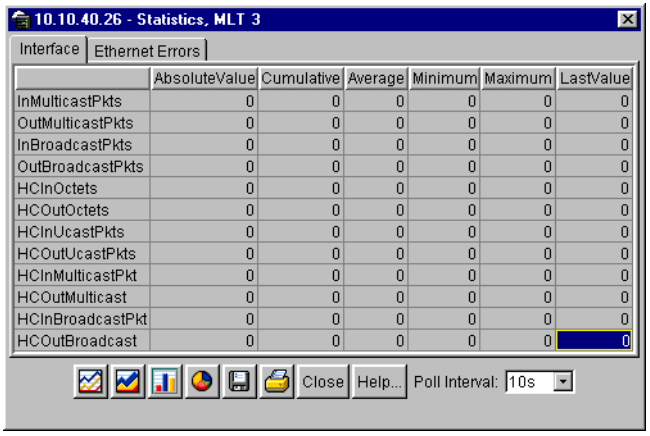


Table 46 describes the fields in the Interface tab.

Table 46 Interface tab fields

Field	Description
InMulticastPkt	The number of packets delivered to this MLT that were addressed to a multicast address at this sublayer. For a MAC layer protocol, this number includes both Group and Functional addresses.
OutMulticast	The total number of packets that higher-level protocols requested be transmitted, and that were addressed to a multicast address at this MLT, including those that were discarded or not sent. For a MAC layer protocol, this number includes both Group and Functional addresses.
InBroadcastPkt	The number of packets delivered to this MLT that were addressed to a broadcast address at this sublayer.
OutBroadcast	The total number of packets that higher-level protocols requested be transmitted, and that were addressed to a broadcast address at this MLT, including those that were discarded or not sent.
HCInOctets	The total number of octets received on the MLT interface, including framing characters.
HCOutOctets	The total number of octets transmitted out of the MLT interface, including framing characters.
HCInUcastPkts	The number of packets delivered by this MLT to higher level protocols that were not addressed to a multicast or broadcast address at this sublayer.

Table 46 Interface tab fields (continued)

Field	Description
HCOutUcastPkts	The number of packets that higher-level protocols requested be transmitted that were not addressed to a multicast address at this MLT.This total number includes those packets discarded or unsent.
HCInMulticastPkt	The number of packets delivered to this MLT that were addressed to a multicast address at this sublayer. For a MAC layer protocol, this number includes both Group and Functional addresses.
HCOutMulticast	The total number of packets that higher-level protocols requested be transmitted, and that were addressed to a multicast address at this MLT, including those that were discarded or not sent. For a MAC layer protocol, this number includes both Group and Functional addresses.
HCInBroadcastPkt	The number of packets delivered to this MLT that were addressed to a broadcast address at this sublayer.
HCOutBroadcast	The total number of packets that higher-level protocols requested be transmitted, and that were addressed to a broadcast address at this MLT, including those that were discarded or not sent.

MultiLink Trunk Ethernet error statistics

To view MultiLink Trunk Ethernet error statistics:

1. From the Device Manager menu bar, choose VLAN > MLT.

   The MLT dialog box opens (Figure 50).

2. Select an MLT by clicking anywhere within a field in the row.
3. Click Graph.

   The Statistics, MLT dialog box opens (Figure 52) with the Interface tab displayed.

4. Click the Ethernet Errors tab.

   The Ethernet Errors tab opens (Figure 53).

Figure 53 MLT Statics dialog box — Ethernet Errors tab

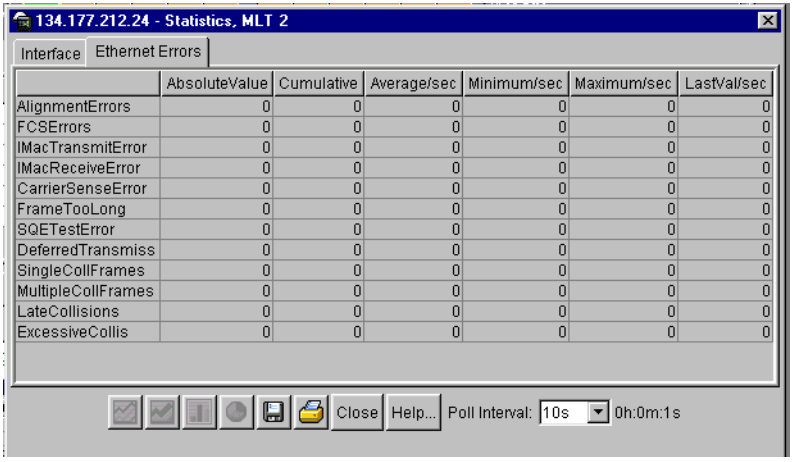

134.177.212.24 - Statistics, MLT 2
Interface
Ethernet Errors
AbsoluteValue
Cumulative
Average/sec
Minimum/sec
Maximum/sec
LastVal/sec
AlignmentErrors 0 0 0 0 0 0
FCSErrors 0 0 0 0 0 0
IMacTransmitError 0 0 0 0 0 0
IMacReceiveError 0 0 0 0 0 0
CarrierSenseError 0 0 0 0 0 0
FrameTooLong 0 0 0 0 0 0
SQETestError 0 0 0 0 0 0
DeferredTransmiss 0 0 0 0 0 0
SingleCollFrames 0 0 0 0 0 0
MultipleCollFrames 0 0 0 0 0 0
LateCollisions 0 0 0 0 0 0
ExcessiveCollis 0 0 0 0 0 0
Close
Help...
Poll Interval:
10s
0h:0m:1s

Table 47 describes the fields in the Ethernet Errors tab.

Table 47 Ethernet Errors tab fields

Field	Description
AlignmentErrors	A count of frames received on a particular MLT that are not an integral number of octets in length and do not pass the FCS check. The count represented by an instance of this object is incremented when the alignmentError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
FCSErrors	A count of frames received on an MLT that are an integral number of octets in length but do not pass the FCS check. The count represented by an instance of this object is incremented when the frameCheckError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
IMacTransmitError	A count of frames for which transmission on a particular MLT fails due to an internal MAC sublayer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the LateCollisions object, the ExcessiveCollisions object, or the CarrierSenseErrors object.
IMacReceiveError	A count of frames for which reception on a particular MLT fails due to an internal MAC sublayer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the FrameTooLongs object, the AlignmentErrors object, or the FCSErrors object. The precise meaning of the count represented by an instance of this object is implementation specific. In particular, an instance of this object may represent a count of receive errors on a particular interface that are not otherwise counted.
CarrierSenseErrors	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular MLT. The count represented by an instance of this object is incremented at most once per transmission attempt, even if the carrier sense condition fluctuates during a transmission attempt.
FrameTooLong	A count of frames received on a particular MLT that exceed the maximum permitted frame size. The count represented by an instance of this object is incremented when the frameTooLong status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.

Table 47 Ethernet Errors tab fields (continued)

Field	Description
SQETestError	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular MLT. The SQE TEST ERROR message is defined in section 7.2.2.2.4 of ANSI/ IEEE 802.3-1985 and its generation is described in section 7.2.4.6 of the same document.
DeferredTransmiss	A count of frames for which the first transmission attempt on a particular MLT is delayed because the medium is busy. The count represented by an instance of this object does not include frames involved in collisions.
SingleCollFrames	A count of successfully transmitted frames on a particular MLT for which transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the MultipleCollisionFrames object.
MultipleCollFrames	A count of successfully transmitted frames on a particular MLT for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the SingleCollisionFrames object.
LateCollisions	The number of times that a collision is detected on a particular MLT later than 512 bit-times into the transmission of a packet. Five hundred and twelve bit-times corresponds to 51.2 microseconds on a 10 Mb/s system. A (late) collision included in a count represented by an instance of this object is also considered as a (generic) collision for purposes of other collision-related statistics.
ExcessiveColls	A count of frames for which transmission on a particular MLT fails due to excessive collisions.

Chapter 5
Creating and managing VLANs

This chapter describes using Device Manager to manage VLANs on your Business Policy Switch 2000. The chapter covers creating, editing, and deleting VLANs. It includes the following sections:

- VLANs (this page)
- Creating VLANs (page 128)
- Modifying and managing existing VLANs (page 138)

VLANs

A VLAN is a collection of ports on one or more switches that define a broadcast domain.The BPS 2000 supports the following three types of VLANs:

- Port-based VLANs (maximum of 256 with software version 1.2)
- Protocol-based VLANs
- Source MAC-based VLANs

For a further description of VLANs, refer to *Using the Business Policy Switch 2000*.

When you create VLANs using Device Manager, observe the following rules:

- The ports in a VLAN or MLT must be a subset of a single spanning tree group.
- VLANs must have unique VLAN IDs and names.
- An access port can belong to one and only one protocol-based VLAN for a given protocol.

- The default VLAN (VLAN ID 1) cannot be renamed or deleted, and it cannot have its type changed from port-based VLAN.

Creating VLANs

Device Manager lets you create port-based, protocol-based, or source address MAC-based VLANs.

Note: After a VLAN is created, you cannot change the VLAN type. The VLAN must be deleted and a new VLAN of the chosen type created.

VLAN information

To open the port-based VLAN dialog box:

➨ From the Device Manager menu bar, choose VLAN > VLANs.

The VLAN dialog box opens with the Basic tab displayed (Figure 54).

Figure 54 VLAN Basic tab

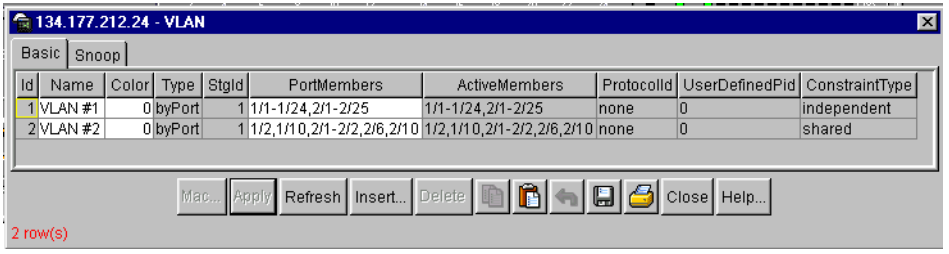


Table 48 describes the Basic tab fields.

Table 48 Basic tab fields

Field	Description
Name	Name of the VLAN.
Color	An administratively-assigned color code for the VLAN. The value of this object is used by the VLAN Manager GUI tool to select a color when it draws this VLAN on the screen.
Type	Indicates the type of VLAN: byPort or byProtocolId.
StgId	Identifies the spanning tree group to which the VLAN belongs.
PortMembers	Ports that are members of the VLAN.
ActiveMember	Set of ports that are currently active in the VLAN. Active ports include all static ports and any dynamic ports where the VLAN policy was met.
ProtocolId	Protocol for protocol-based VLANs. This value is taken from the Assigned Numbers RFC. For port-based VLANs, none is the displayed value.
UserDefinedPid	When rcVlanProtocolId is set to usrDefined(15) in a protocol-based VLAN, this field represents the 16-bit user defined protocol identifier.
ConstraintType	Displays whether the specified VLAN is independent or shared.

Creating a port-based VLAN

To create a port-based VLAN:

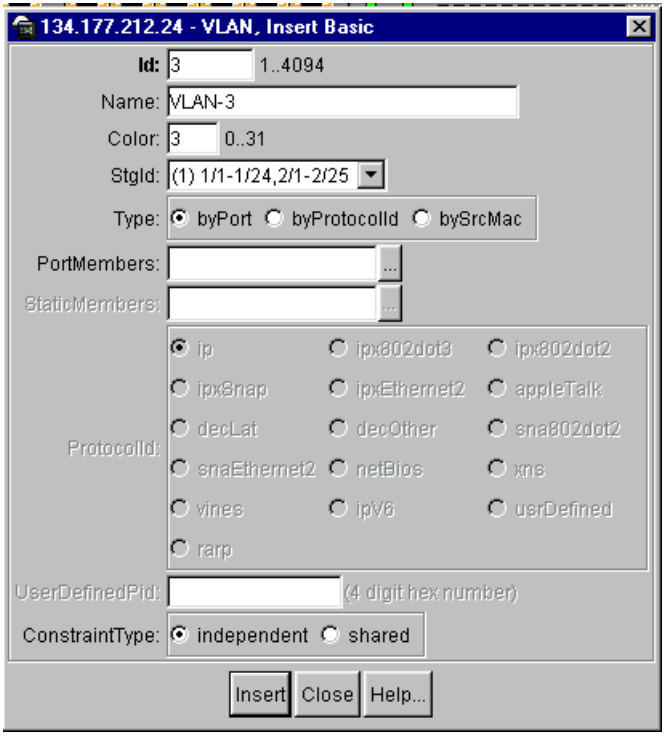
1 From the Device Manager menu bar, choose VLAN > VLANs.

The VLAN dialog box opens (Figure 54).

2 Click Insert.

The Insert Basic dialog box for creating VLANs opens (Figure 55). This dialog box opens with the Type field set to byPort.

Figure 55 VLAN, Insert Basic dialog box for a port-based VLANs


134.177.212.24 - VLAN, Insert Basic
Id: 3 1..4094
Name: VLAN-3
Color: 3 0..31
StgId: (1) 1/1-1/24,2/1-2/25
Type: byPort byProtocolId bySrcMac
PortMembers:
StaticMembers:
ProtocolId: ip ipx802dot3 ipx802dot2 ipxSnap ipxEthernet2 appleTalk decLat decOther sna802dot2 snaEthernet2 netBios xns vines ipV6 userDefined rarp
UserDefinedPid: (4 digit hex number)
ConstraintType: independent shared
Insert Close Help...

3 Type the VLAN ID.

The value can be from 1 to 4094, as long as it is not already in use. (The default VLAN has a VID=1.)

4 Type the VLAN name (optional).

If no name is entered, a default name is created.

5 Enter a color ID for the VLAN (optional).

6 Use the StgId menu to choose the Spanning Tree group to which the VLAN is to belong.

7 In the Type field, click byPort if not already selected.

8 Specify the port membership by clicking the PortMembers buttons.

Note: You can add ports that are also members of other VLANs within the same STG. However, you cannot add ports that are members of a VLAN that is within a different STG.

9 In the ConstraintType field, click independent or shared.

10 Click Insert.

Creating a protocol-based VLAN

To create a protocol-based VLAN:

1 From the Device Manager menu bar, choose VLAN > VLANs.

The VLAN dialog box opens (Figure 54).

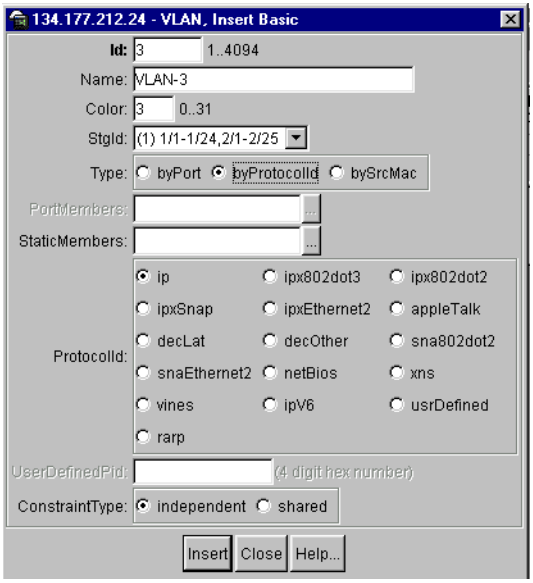
2 Click Insert.

The Insert Basic dialog box for creating VLANs opens (Figure 55).

3 Change the Type field to byProtocolID.

The dialog box changes to display additional fields needed to set up protocol-based VLANs (Figure 56).

Figure 56 VLAN, Insert Basic dialog box for a protocol-based VLAN


134.177.212.24 - VLAN, Insert Basic
Id: 3 1..4094
Name: VLAN-3
Color: 3 0..31
StgId: (1) 1/1-1/24,2/1-2/25
Type: byPort byProtocolId bySrcMac
PortMembers:
StaticMembers:
ProtocolId: ip ipx802dot3 ipx802dot2 ipxSnap ipxEthernet2 appleTalk decLat decOther sna802dot2 snaEthernet2 netBios xns vines ipV6 usrDefined rarp
UserDefinedPid: (4 digit hex number)
ConstraintType: independent shared
Insert Close Help...

4 Type the unique VLAN ID.

5 Type the VLAN name (optional).

If no name is entered, the protocol name becomes the default VLAN name.

6 Enter a color ID for the VLAN (optional).

7 Use the StgId menu to choose the Spanning Tree group to which the VLAN is to belong.

8 In the Type field, click byProtocolID if not already selected.

9 Specify Static Members by clicking the ellipsis (...) field.

Note: You can add ports that are also members of other VLANs within the same STG. However, you cannot add ports that are members of a VLAN that is within a different STG.

10 In the ProtocolID field select one protocol radio button.

11 In the ConstraintType field, click independent or shared.

12 Click Insert.

Note: For protocol-based VLANs, you can have up to 14 table entries.

Creating a source address MAC-based VLAN

To create a source address MAC-based VLAN:

1 From the Device Manager menu bar, choose VLAN > VLANs.

The VLAN dialog box opens (Figure 54).

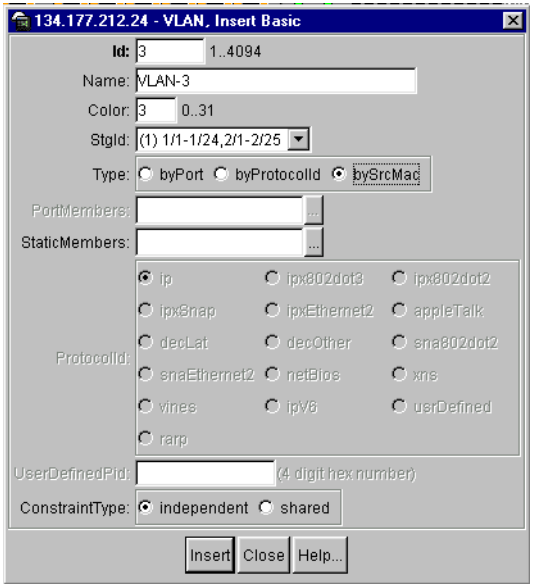
2 Click Insert.

The VLAN, Insert Basic dialog box opens (Figure 57). This dialog box opens with the Type field set to byPort.

3 Change the Type field to bySrcMac.

The dialog box changes to display additional fields needed to set up source MAC-based VLANs (Figure 57).

Figure 57 VLAN, Insert Basic dialog box for a source MAC-based VLAN


134.177.212.24 - VLAN, Insert Basic
Id: 3 1..4094
Name: VLAN-3
Color: 3 0..31
StgId: (1) 1/1-1/24,2/1-2/25
Type: byPort byProtocolId bySrcMac
PortMembers:
StaticMembers:
ProtocolId: ip ipx802dot3 ipx802dot2 ipxSnap ipxEthernet2 appleTalk decLat decOther sna802dot2 snaEthernet2 netBios xns vines ipV6 userDefined rarp
UserDefinedPid: (4 digit hex number)
ConstraintType: independent shared
Insert Close Help...

4 Enter the unique VLAN ID.

5 Enter the VLAN name (optional).

If no name is entered, the protocol name becomes the default VLAN name.

6 Enter a color ID for the VLAN (optional).

7 Use the StgId menu to choose the Spanning Tree group to which the VLAN is to belong.

8 In the Type field, click bySrcMac if not already selected.

9 Specify the static membership by clicking the ellipsis (...) field.

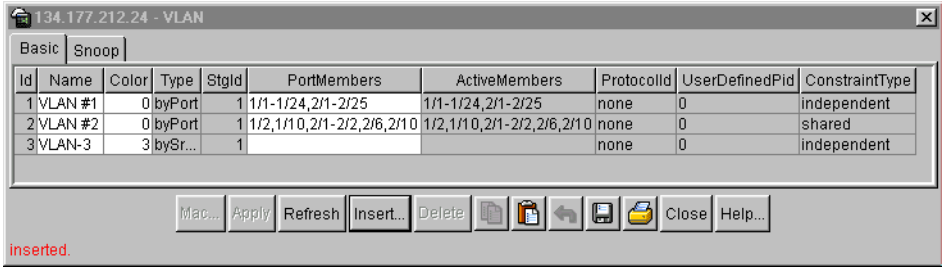
Note: You can add ports that are also members of other VLANs within the same STG. However, you cannot add ports that are members of a VLAN that is within a different STG.

10 In the ConstraintType field, click independent or shared.

11 Click Insert.

The VLAN dialog box opens (Figure 58).

Figure 58 VLAN dialog box

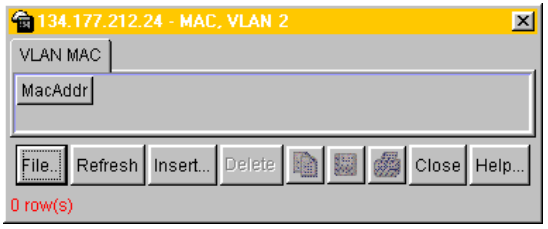


12 Highlight the BySrcMac field.

13 Click MAC.

The MAC, VLAN dialog box opens (Figure 59).

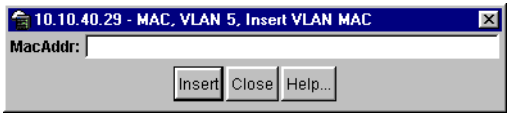
Figure 59 MAC, VLAN dialog box



14 Click Insert

The Insert VLAN MAC dialog box opens (Figure 60).

Figure 60 Insert VLAN MAC dialog box



15 Type the source MAC address for the VLAN.

16 Click Insert.

Note: In a source MAC-based VLAN, a potential member becomes an active member of the VLAN when a frame with the specified source MAC address is received. Source MAC-based VLANs are not supported in a mixed stack environment.

Accepting tagged and untagged frames

In the Business Policy Switch, you configure whether or not tagged frames are sent or received on the port level. Refer to "VLAN tab for a single port" on page 89 for VLAN tab field descriptions. Tagging is set as true or false for the port and applied to all VLANs on that port. You can select whether or not to discard:

- Tagged frames received on a port where tagging is disabled
- Untagged frames received on a port where tagging is enabled

The default is not to discard the frames. You can also designate the port-based VLAN to which these frames are assigned by setting the tagged port's default VID (the default is 1).

A Business Policy Switch switch port with tagging enabled is a port from which all frames sent are tagged. A tagged port can be configured to discard untagged frames or to associate them with a VLAN set by the PVID. In the latter case, when an untagged frame is received on a tagged port, it is sent to the user-specified PVID.

A port with tagging disabled is a port that does not send tagged frames. If a tagged frame is forwarded out a port with tagging set to false, the switch removes the tag from the frame before sending it out the port. When a port with tagging set to false receives a frame, it can be configured to discard tagged frames or to associate them with the VLAN specified in the tag.

Note: To optimize performance, on untagged ports in configurations where you do not expect to see tagged frames, set DiscardTaggedFrames to true. However, on untagged ports for interconnecting switches, it is probably better to set DiscardTaggedFrames to false. Then, if you convert an interswitch port from an untagged port to a tagged port, connectivity is not lost.

To set a port to discard tagged frames it receives:

1. In the Device Manager main window, select a port.
2. From the Device Manager menu bar, choose Edit > Port.

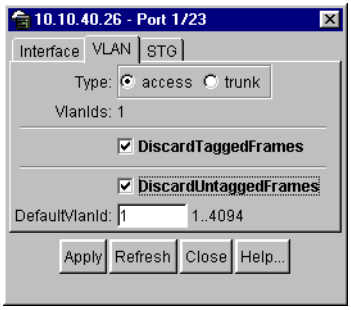
   The Port dialog box opens displaying the Interface tab.

3 Click the VLAN tab.

The VLAN tab opens (Figure 61).

Select the DiscardTaggedFrames and the DiscardUntaggedFrames check boxes.

Figure 61 VLAN tab



4 Click Apply.

Snoop tab

You can use the Snoop tab to enable or disable VLAN snooping on a switch.

To open the port-based VLAN:

1 From the Device Manager menu bar, choose VLAN > VLANs.

The VLAN dialog box opens (Figure 54) with the Basic tab displayed.

2 Click the Snoop tab.

The Snoop tab opens (Figure 62).

Figure 62 Snoop tab

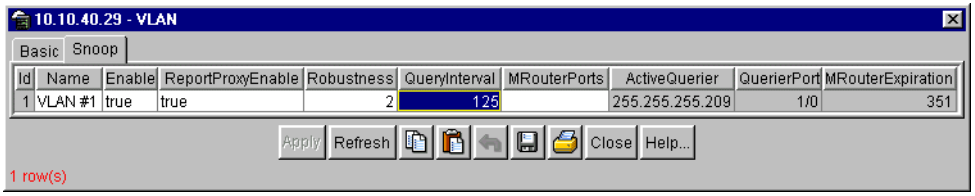


Table 49 describes the Snoop tab fields.

Table 49 Snoop tab fields

Field	Description
Name	Name of the VLAN.
Enable	Sets whether IGMP snooping is enabled or disabled.
ReportProxyEnable	Sets whether IGMP report proxy is enabled or disabled.
Rebustness	Allows tuning for the expected packet loss on a subnet. If a subnet is expected to be bad, the Robustness variable can be increased. IGMP is robust to packet losses.
QueryInterval	Intervals (in seconds) between IGMP host and query packets transmitted on an interface.
MRouterPorts	A set of ports in the VLAN that provide connectivity to an IP multicast router.
ActiveQuerier	This is the IP address of a multicast querier router.
QuerierPort	The port that the multicast querier router was heard.
MRouterExpiration	The multicast querier router aging that will be timed out.

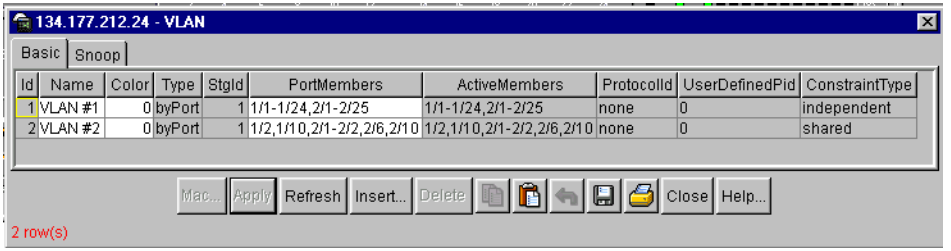
Modifying and managing existing VLANs

The main dialog box for managing VLANs in Device Manager is the VLAN dialog box. To open the VLAN dialog box:

➨ From the Device Manager main menu, choose VLAN > VLANs.

The VLAN dialog box opens (Figure 63). The VLAN dialog box displays all defined VLANs, their configurations, and their current status.

Figure 63 VLAN dialog box



Note: After a VLAN is created, you cannot change the VLAN type. The VLAN must be deleted and a new VLAN of the chosen type created.

Table 50 describes the fields in the VLAN dialog box.

Table 50 VLAN dialog box fields

Field	Description
Id	The VLAN ID for the VLAN (unlabeled farthest left column).
Name	The name of the VLAN.
Color	The color used, for visual purposes only, by VLAN Manager to associate a color with a VLAN. The assigned color does not affect the behavior of a frame, only the attributes assigned to the VLAN.
Type	Indicates the type of VLAN: byPort or byProtocolId.
StgId	The spanning tree group ID to which the VLAN belongs.
PortMembers	The ports that are members of the VLAN.
ActiveMembers	The ports that are members of the VLAN.
ProtocolId	The protocol for protocol-based VLANs. This value is taken from the Assigned Numbers RFC. For port-based VLANs, none is the displayed value.
UserDefined	When rcVlanProtocolId is set to usrDefined(15) in a protocol-based VLAN, this field represents the 16-bit user defined protocol identifier.
ConstraintType	Displays whether the specified VLAN is independent or shared.

Deleting LANs

To delete a VLAN:

1. From the Device Manager menu bar, choose VLAN > VLANs.

   The VLAN dialog box opens (Figure 54).

2. Select the VLAN that you want to delete.
3. Click Delete.

   Device Manager deletes the selected VLAN.

Chapter 6
Creating and managing multiple STGs

This chapter describes using Device Manager to manage multiple Spanning Tree Groups (STGs) on your Business Policy Switch 2000. With software version 1.2 and later, the BPS 2000 supports multiple STGs. This chapter includes the following sections:

- "STGs," next
- "Configuring STGs" on page 142
- "Deleting an STG configuration" on page 146
- "Displaying STG status" on page 147
- "Displaying STG ports" on page 148

STGs

The BPS 2000 supports a maximum of 8 multiple STGs, either all in one standalone switch or across a stack.When working with STGs, observe the following rules:

- Enable load balancing using multiple STGs by configuring each path with a different VLAN and then assigning each VLAN to a separate STG**.**
- Each STG must be independently configured.
- With software version 1.2 and later, the BPS 2000 supports a maximum of 256 port-based VLANs. With a maximum of 8 STGs, on average, each STG will have 32 VLANs.
- In the default configuration of the BPS 2000, a single STG with the ID of 1 includes all ports on the switch.
  - The Default STG sends only untagged BPDUs in order to operate with all devices that support only one instance of STP.

  - Although ports can be added to or deleted from the Default STG, the Default STG itself cannot be deleted from the system.
- All other STGs must be created by the user.
- An STG cannot be deleted until you disable it. Additionally, you cannot delete an STG while it contains VLAN members, so you must first delete the VLANs from the STG.
- The ports associated with a VLAN and VLANs themselves must be contained **within** a single STG.
- When a VLAN spans multiple switches, the VLAN must be within the same spanning tree group (have the STG ID) across all the switches.
- When a VLAN is assigned to an STG, all ports belonging to that VLAN automatically join the STG. And, all VLANs in the same shared database (SVL) must be assigned to the same STG.
- All members of a particular MultiLink Trunking (MLT) group must be assigned to the same STG.
- Tagged ports can belong to more than one STG, but untagged ports can belong to **only one** STG.
  - When a tagged port belongs to more than one STG, the egress BPDUs are tagged to distinguish the BPDUs of one STG from those of another STG. BPDUs from STG 1 (the Default STG) are untagged.
  - Because some STP-compliant devices do not support tagging, you can configure whether to send tagged or untagged BPDUs, even from tagged ports, with the BPS 2000 with software version 1.2. The VLAN ID for the tagged BPDUs will be 4000+STG ID.

Note: You cannot remove VLAN 1 from spanning tree group (STG) 1.

Configuring STGs

This section contains the following procedures:

- "Viewing STG configuration," next
- "Creating an STG" on page 144
- "Adding a VLAN to an STG" on page 146

- "Moving a VLAN between STGs" on page 146

Viewing STG configuration

Use the STG dialog box to view the current STG configuration.

To open the STG dialog box:

➡ From the Device Manager menu bar, choose VLAN > STG.

The STG dialog box opens with the Configuration tab displayed (Figure 64).

Figure 64 STG Configuration tab

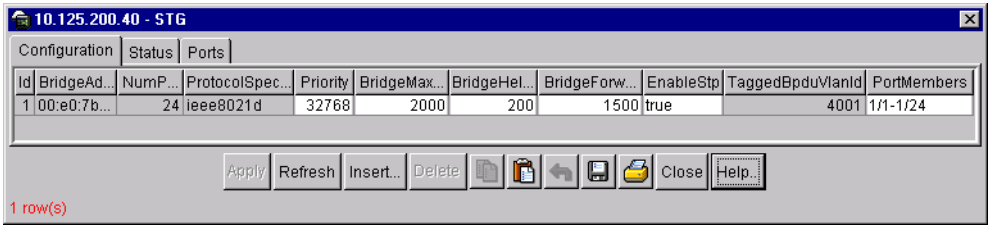


Table 51 describes the Configuration tab of the STG dialog box.

Table 51 Configuration tab fields

Field	Description
Id	Displays an integer between 1 and 8 that identifies the STG.
BridgeAddress	Displays the MAC address used by this bridge; usually the smallest MAC address of all ports in the bridge.
NumPorts	Displays the number of ports controlled by this bridging entity.
ProtocolSpecification	Displays the version of spanning tree that is running.
Priority	Enter the first two octets of the 8-octet bridge ID; range is 0 to 65535.
BridgeMaxAge	Enter the maximum time you want to allow before the specified STG times out, in seconds; range is 600 to 4,000.
BridgeHelloTime	Enter the maximum time between hellos, in seconds; range is 100 to 1,000.

Table 51 Configuration tab fields (continued)

Field	Description
BridgeForwardDelay	Enter the maximum delay in forwarding, in seconds; range is 400 to 3,000.
Enable STP	Lets you enable or disable the spanning tree group.
TaggedBdpuVlanId	The VLAN ID for tagged BDPUs.
PortMembers	Displays which ports are members of the specified STG. Although this field is read-write, the Business Policy Switch 2000 does not support adding or removing ports directly to STGs. Instead, you must change the port membership by adding and removing VLANs.

Creating an STG

Device Manager lets you create STGs.

Note: The Business Policy Switch 2000 only supports multiple STGs when it is in pure stack mode. When configured for hybrid stack mode, the device only supports one STG. To change the stack mode, see *Using the Business Policy Switch 2000 Version 2.0*.

To create an STG:

1 From the Device Manager menu bar, choose VLAN > STGs.

The STG Configuration dialog box opens (Figure 64).

2 Click Insert.

The Insert Configuration dialog box for creating STGs opens (Figure 65).

Figure 65 STG, Insert Configuration dialog box

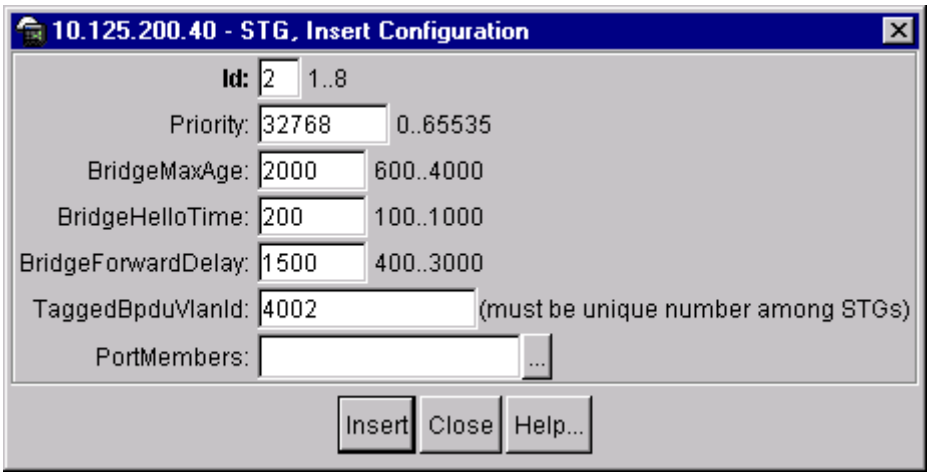


Table 52 describes the STG, Insert Configuration tab fields.

Table 52 STG, Insert Configuration tab fields

Field	Description
Id	Enter an integer between 1 and 25 that identifies the STG; 1 is the default STG.
Priority	Enter the first two octets of the 8-octet bridge ID; range is 0 to 65535.
BridgeMaxAge	Enter the maximum time you want to allow before the specified STG times out, in seconds; range is 600 to 4,000.
BridgeHelloTime	Enter the maximum time between hellos, in seconds; range is 100 to 1,000.
BridgeForwardDelay	Enter the maximum delay in forwarding, in seconds; range is 400 to 3,000.
TaggedBdpuVlanId	Enter the VLAN ID for tagged BDPUs.
PortMembers	Opens a dialog box that lets you specify ports as members of the specified STG for some BayStack and Passport devices. Do not use this feature with the Business Policy Switch 2000 The Business Policy Switch 2000 does not support adding or removing ports directly to STGs. Instead, you must change the port membership by adding and removing VLANs.

Adding a VLAN to an STG

When using Device Manager, you can only add VLANs to an STG at the time you are creating the VLAN.

To add a VLAN to an STG:

1. If it does not already exist, create the STG to which you want to add the VLAN.

   See "Creating an STG" on page 144 for more information about creating STGs.

2. Create the VLAN, making sure to select the desired StgId on the Insert VLAN dialog box.

   See "Creating VLANs" on page 128 for more information about creating VLANs.

3. Open the STG dialog box, and view the Configuration tab to confirm that the ports of the new VLAN were added to the STG.

Moving a VLAN between STGs

Device Manger does not let you move VLANs between STGs on the Business Policy Switch 2000. Instead, you must delete the VLAN that you want to move, and add a replacement VLAN in the STG to which you want to move the VLAN.

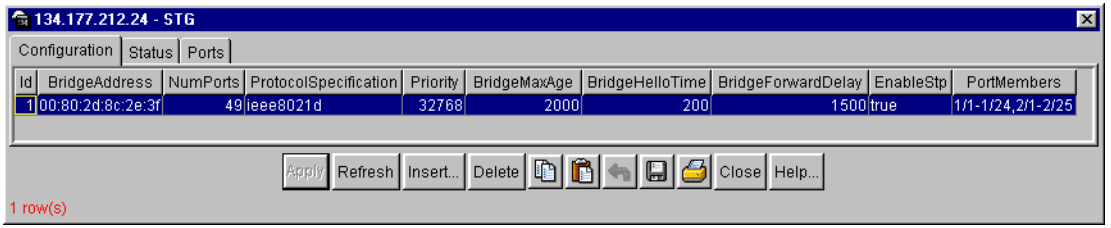
For information on deleting VLANs, see "Deleting LANs" on page 139. For information on adding VLANs to STGs, see "Adding a VLAN to an STG" on page 146.

Deleting an STG configuration

To delete an STG configuration:

1. In the Configuration tab of the STG dialog box, select an STG or multiple STGs.

Figure 66 STG Configuration tab - Highlighted configuration fields



2 Click the delete button.

Note: You cannot delete the default spanning tree group (STG) 1.

Displaying STG status

To display the status of STGs:

1 From the Device Manager menu bar, choose VLAN > STGs.

The STG dialog box opens with the Configuration tab displayed (Figure 64).

2 Click the Status tab.

The Status tab opens (Figure 67).

Figure 67 Status tab

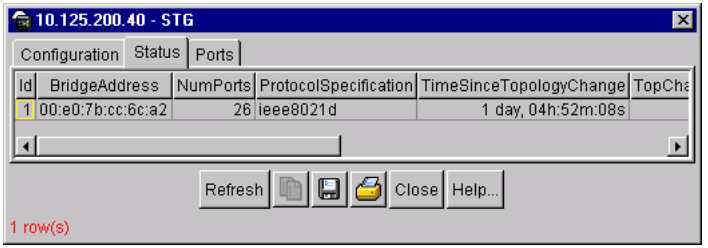


Table 53 describes the Status tab fields.

Table 53 Status tab fields

Field	Description
Id	Displays the STG ID.
BridgeAddress	Displays the MAC address used by this bridge.
NumPorts	Displays the number of ports controlled by this bridging entity.
ProtocolSpecification	Displays the version of spanning tree that is running.
TimeSinceTopologyChange	Displays the time, in hundredths of seconds, since the last topology change.
TopChanges	Displays number of topology changes since switch was reset.
DesignatedRoot	Displays MAC address of designated root of STP.
RootCost	Displays the cost of the path to the root.
RootPort	Displays the port number of the port with the lowest-cost path from this bridge to the root bridge.
MaxAge	Displays the maximum age, in hundredths of a second, of STP information learned from any port in the network before information is discarded.
HelloTime	Displays the amount of time, in hundredths of seconds, between Hello messages.
HoldTime	Displays interval, in hundredths of seconds, during which no more than 2 Hello messages can be transmitted.
ForwardDelay	Displays interval, in hundredths of seconds, the switch currently stays in Listening or Learning mode, before moving to Forwarding mode. this value is also used to age dynamic entries in the Forwarding Database.

Displaying STG ports

To display the STG port status:

1 From the Device Manager menu bar, choose VLAN > STGs.

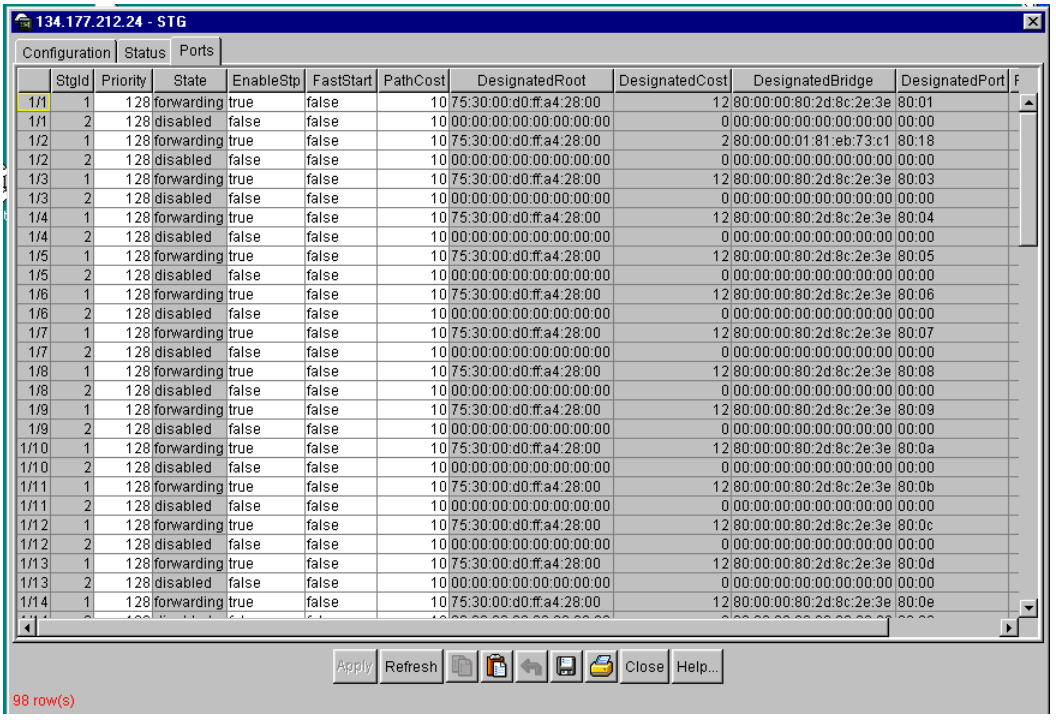
The STG dialog box opens with the Configuration tab displayed (Figure 64).

2 Click the Ports tab.

The Ports tab opens (Figure 68).

3 View the information and, if desired, change the information in the Ports tab by entering information and using the pull-down menus.

Figure 68 Ports tab



	StgId	Priority	State	EnableStp	FastStart	PathCost	DesignatedRoot	DesignatedCost	DesignatedBridge	DesignatedPort
1/1	1	128	forwarding	true	false	10	75:30:00:d0:ff:a4:28:00	12	80:00:00:80:2d:8c:2e:3e	80:01
1/1	2	128	disabled	false	false	10	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00
1/2	1	128	forwarding	true	false	10	75:30:00:d0:ff:a4:28:00	2	80:00:00:01:81:eb:73:c1	80:18
1/2	2	128	disabled	false	false	10	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00
1/3	1	128	forwarding	true	false	10	75:30:00:d0:ff:a4:28:00	12	80:00:00:80:2d:8c:2e:3e	80:03
1/3	2	128	disabled	false	false	10	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00
1/4	1	128	forwarding	true	false	10	75:30:00:d0:ff:a4:28:00	12	80:00:00:80:2d:8c:2e:3e	80:04
1/4	2	128	disabled	false	false	10	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00
1/5	1	128	forwarding	true	false	10	75:30:00:d0:ff:a4:28:00	12	80:00:00:80:2d:8c:2e:3e	80:05
1/5	2	128	disabled	false	false	10	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00
1/6	1	128	forwarding	true	false	10	75:30:00:d0:ff:a4:28:00	12	80:00:00:80:2d:8c:2e:3e	80:06
1/6	2	128	disabled	false	false	10	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00
1/7	1	128	forwarding	true	false	10	75:30:00:d0:ff:a4:28:00	12	80:00:00:80:2d:8c:2e:3e	80:07
1/7	2	128	disabled	false	false	10	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00
1/8	1	128	forwarding	true	false	10	75:30:00:d0:ff:a4:28:00	12	80:00:00:80:2d:8c:2e:3e	80:08
1/8	2	128	disabled	false	false	10	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00
1/9	1	128	forwarding	true	false	10	75:30:00:d0:ff:a4:28:00	12	80:00:00:80:2d:8c:2e:3e	80:09
1/9	2	128	disabled	false	false	10	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00
1/10	1	128	forwarding	true	false	10	75:30:00:d0:ff:a4:28:00	12	80:00:00:80:2d:8c:2e:3e	80:0a
1/10	2	128	disabled	false	false	10	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00
1/11	1	128	forwarding	true	false	10	75:30:00:d0:ff:a4:28:00	12	80:00:00:80:2d:8c:2e:3e	80:0b
1/11	2	128	disabled	false	false	10	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00
1/12	1	128	forwarding	true	false	10	75:30:00:d0:ff:a4:28:00	12	80:00:00:80:2d:8c:2e:3e	80:0c
1/12	2	128	disabled	false	false	10	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00
1/13	1	128	forwarding	true	false	10	75:30:00:d0:ff:a4:28:00	12	80:00:00:80:2d:8c:2e:3e	80:0d
1/13	2	128	disabled	false	false	10	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00
1/14	1	128	forwarding	true	false	10	75:30:00:d0:ff:a4:28:00	12	80:00:00:80:2d:8c:2e:3e	80:0e

Table 54 describes the Ports tab fields.

Table 54 Ports tab fields

Field	Description
	Displays the unit and port number.
StgId	Displays the STG ID number.
Priority	Specifies the port priority
State	Displays STP state of the port: Disabled, Blocking, Listening, Learning, Forwarding.
EnableStp	Use the pull-down menu to enable or disable STP on the port: true is enabled, and false is disabled.
FastStart	Use the pull-down menu to enable or disable Fast Start STP on the port: true is enabled, and false is disabled.
PathCost	Displays or enters the contribution of this port to the cost path of the spanning tree root.
DesignatedRoot	Displays MAC address of designated root of STP.
DesignatedCost	Displays the path cost of the designated port of the segment connected to this port.
DesignatedBridge	Displays MAC address of designated bridge this port considers designated bridge for this segment.
DesignatedPort	Displays the port ID on the designated bridge for this port's segment.
ForwardTransitions	Displays the number of times port transitioned from STP Learning to Forwarding state.

Chapter 7
Configuring QoS

This chapter describes using Device Manager to manage Quality of Service (QoS) parameters on your Business Policy Switch 2000. Additionally, this chapter describes using Common Open Policy Services (COPS). It includes the following sections:

- Managing interface groups
- Managing QoS rules
- Managing QoS actions, meters, shapers, and policies
- QoS agent
- COPS overview

See chapters 3, 4, and 5 of *Using the Business Policy Switch 2000 Version 2.0* for a detailed description of Quality of Service (QOS) parameters.

Managing interface groups

You can display interface queues and groups.

Displaying interface queues

To display interface queues:

➨ From the Device Manager menu bar, choose QoS/COPS > QoS Devices.

The QoSDevice dialog box opens with the Interface Queue tab displayed (Figure 69).

Figure 69 Interface Queue tab

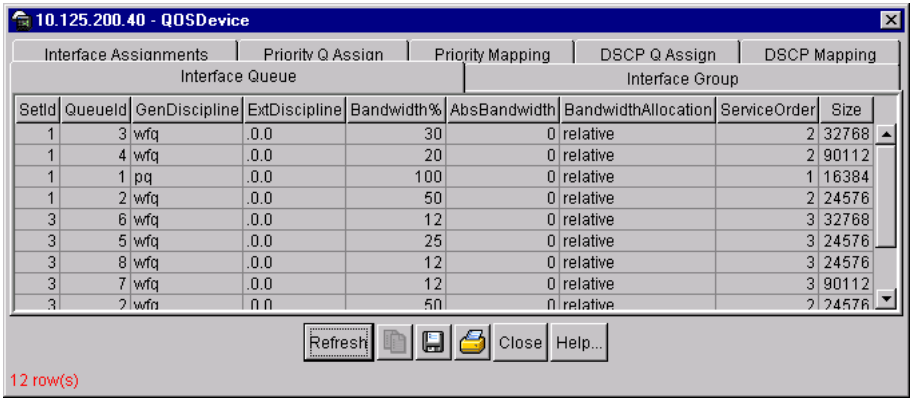

10.125.200.40 - QOSDevice
Interface Assignments
Priority Q Assign
Priority Mapping
DSCP Q Assign
DSCP Mapping
Interface Queue
Interface Group
SetId QueueId GenDiscipline ExtDiscipline Bandwidth% AbsBandwidth BandwidthAllocation ServiceOrder Size
1 3 wfq .0.0 30 0 relative 2 32768
1 4 wfq .0.0 20 0 relative 2 90112
1 1 pq .0.0 100 0 relative 1 16384
1 2 wfq .0.0 50 0 relative 2 24576
3 6 wfq .0.0 12 0 relative 3 32768
3 5 wfq .0.0 25 0 relative 3 24576
3 8 wfq .0.0 12 0 relative 3 24576
3 7 wfq .0.0 12 0 relative 3 90112
Refresh
Close
Help...
12 row(s)

Table 55 describes the Interface Queue tab fields.

Table 55 Interface Queue tab fields

Field	Description
SetId	Displays an integer between 1 and 65535 that identifies the specific queue set.
QueueId	Displays an integer that uniquely identifies a specific queue within a set of queues.
GenDiscipline	Displays the paradigm used to empty the queue: • other-Refer to ExtDiscipline • fifo-first in, first out queuing • pq-priority queuing • fq-fair queuing (round-robin) • wfq-weighted fair queuing
ExtDiscipline	The queueing discipline that is associated with the specified queue. This attribute provides a means to add more queueing mechanisms.
Bandwidth%	Displays relative bandwidth available to a given queue with respect to other associated queues.
AbsBandwidth	Displays absolute bandwidth available to this queue, in Kb/s.
BandwidthAllocation	Displays bandwidth allocation: relative or absolute.
ServiceOrder	The order in which a a queue is serviced based on the defined discipline.
Size	Displays the size of the queue in bytes.

Displaying interface groups

To display interface groups:

1 From the Device Manager menu bar, choose QoS/COPS > QoS Devices.

The QoSDevice dialog box opens with the Interface Queue tab displayed (Figure 69).

2 Click the Interface Group tab.

The Interface Group tab opens (Figure 70).

Figure 70 Interface Group tab

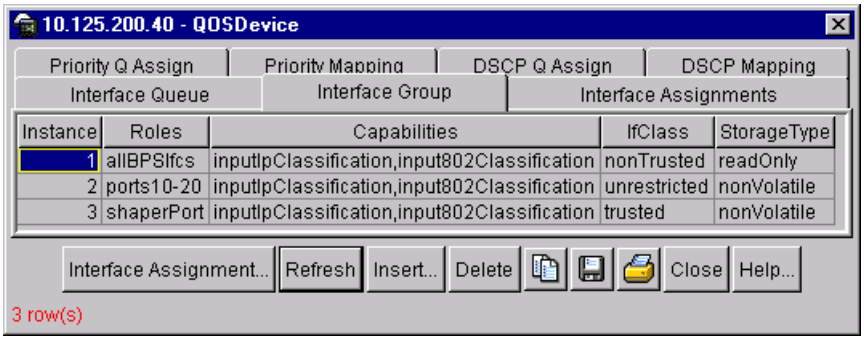


Table 56 describes the Interface Group tab fields.

Table 56 Interface Group tab fields

Field	Description
Id	Displays a unique identifier of an interface group.
Roles	The tag used to identify interfaces with the characteristics specified by the attributes of this class instance. These identifiers can be used within a number of classes to identify a physical set of interfaces to which policy rules and actions can apply.
Capabilities	A list of the interface capabilities used by the PDP or network manager to select the policies and configurations that can be pushed to the Policy Enforcement Point (PEP).

Table 56 Interface Group tab fields (continued)

Field	Description
IfClass	The type of traffic received on interfaces associated with the specified role combination.
StorageType	Displays storage type for this interface group: • Volatile • nonVolatile (default) • readOnly

Assigning ports to an interface group

To assign ports to an interface group:

1 From the Device Manager menu bar, choose QoS/COPS > QoS Devices.

The QoSDevice dialog box opens with the Interface Queue tab displayed (Figure 69).

2 Click the Interface Group tab.

The Interface Group tab opens (Figure 70).

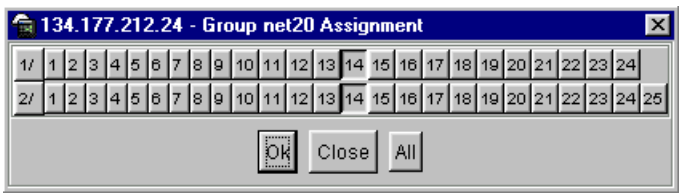
3 Highlight the interface group you want to add ports to.

The Interface Assignment button appears on the bottom of the tab.

4 Click Interface Assignment.

The Group Assignment dialog box opens (Figure 71).

Figure 71 Group Assignment dialog box



5 Click the port numbers you want to add to the interface group.

6 Click OK.

Note: Adding or deleting a number of ports can take a long time, and may cause the Device Manager to time out.

Deleting ports from an interface group

To remove ports from an interface group:

1 From the Device Manager menu bar, choose QoS/COPS > QoS Devices.

The QoSDevice dialog box opens with the Interface Queue tab displayed (Figure 69).

2 Click the Interface Group tab.

The Interface Group tab opens (Figure 70).

3 Highlight the interface group you want to delete ports from.

The Interface Assignment button appears on the bottom of the tab.

4 Click Interface Assignment.

The Group Assignment dialog box opens (Figure 71).

5 Click the port numbers you want to delete from the interface group.

6 Click OK.

Adding interface groups

To add an interface group:

1 From the Device Manager menu bar, choose QoS/COPS > QoS Devices.

The QoSDevice dialog box opens with the Interface Queue tab displayed (Figure 69).

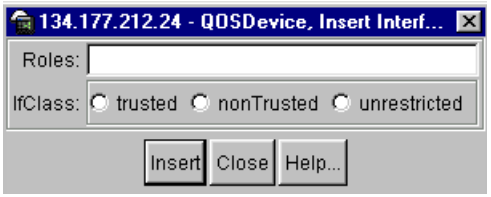
2 Click the Interface Group tab.

The Interface Group tab opens (Figure 70).

3 Click Insert.

The Insert Interface Group dialog box opens (Figure 72).

Figure 72 Insert Interface Group dialog box



4 Enter the Role combination tag you want for this Interface Group.

5 Choose the interface class you want for this interface group: trusted, nonTrusted, or unrestricted.

6 Click Insert.

Deleting interface groups

To delete an interface group:

1 From the Device Manager menu bar, choose QoS/COPS > QoS Devices.

The QoSDevice dialog box opens with the Interface Queue tab displayed (Figure 69).

2 Click the Interface Group tab.

The Interface Group tab opens (Figure 70).

3 Highlight the interface group you want to delete.

4 Click Delete.

Note: You cannot delete an interface group that is referenced by a policy. You must first delete the policy. You also cannot delete an interface group that has ports assigned to it.

You can display the association between interfaces, role combinations, and queue sets. A role combination is a unique label that identifies a group of interfaces.

Displaying interface IDs

To display the interface ID:

1 From the Device Manager menu bar, choose QoS/COPS > QoS Devices.

The QoSDevice dialog box opens with the Interface Queue tab displayed (Figure 69).

2 Click the Interface Assignments tab.

The Interface Assignments tab opens (Figure 73).

The table may take awhile to fill, and you can interrupt the process by clicking the Stop button. The Stop button disappears when the table is complete

Figure 73 Interface Assignments tab

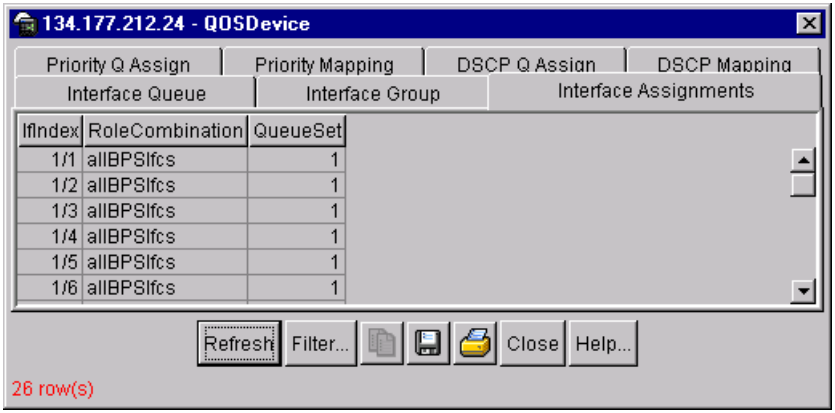


Table 57 describes the Interface Assignments tab fields.

Table 57 Interface Assignments tab fields

Field	Description
IfIndex	Displays ports numbers.

Table 57 Interface Assignments tab fields (continued)

Field	Description
RoleCombination	Displays the role combination associated with the interface.
QueueSet	Displays the queue set associated with this interface.

Displaying priority queue assignments

To display priority queue assignments:

1 From the Device Manager menu bar, choose QoS/COPS > QoS Devices.

The QoSDevice dialog box opens with the Interface Queue tab displayed (Figure 69).

2 Click the Priority Q Assign tab.

The Priority Q Assign tab opens (Figure 74).

Figure 74 Priority Q Assign tab

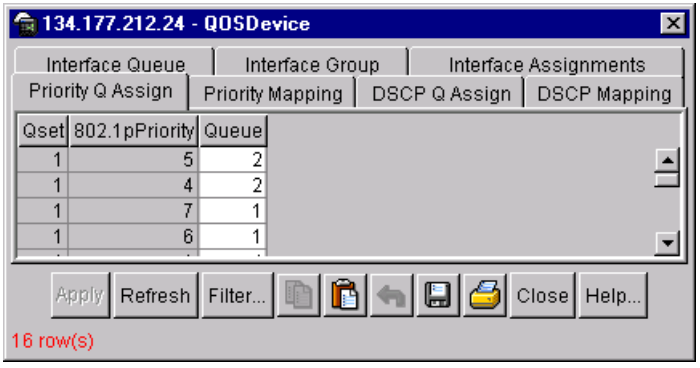


Table 58 describes the Priority Q Assign tab fields.

Table 58 Priority Q Assign tab fields

Field	Description
Qset	Supports the assignment of 802.1p user priority values to a queue for each specific queue set. There will be 8 instances of this class for each supported queue set.
802.1pPriority	A 802.1 user priority value.
Queue	A queue in a specified queue set that is assigned a priority value. To change a Queue assignment, click in the cell and type a new value.

Displaying priority mapping

To display priority mapping:

1 From the Device Manager menu bar, choose QoS/COPS > QoS Devices.

The QoSDevice dialog box opens with the Interface Queue tab displayed (Figure 69).

2 Click the priority mapping tab.

The priority mapping tab opens (Figure 75).

Figure 75 Priority mapping tab

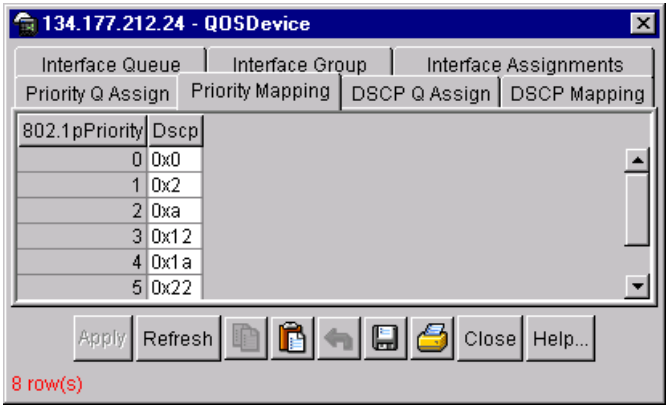


Table 59 describes the priority mapping tab fields.

Table 59 Priority mapping tab fields

Field	Description
802.1pPriority	A 802.1 user priority value to map to a DSCP value at ingress.
Dscp	A DSCP value to associate with the specified 802.1 user priority value at ingress. To change a DSCP assignment, double-click in a Dscp cell and edit the value.

Displaying DSCP queue assignments

To display DSCP Queue assignments:

1 From the Device Manager menu bar, choose QoS/COPS > QoS Devices.

The QoSDevice dialog box opens with the Interface Queue tab displayed (Figure 69).

2 Click the DSCP Q Assign tab.

The DSCP Q Assign tab opens (Figure 76).

Figure 76 DSCP Q Assign tab

Table 60 describes the DSCP Q Assign tab fields. All fields are read-only.

Table 60 DSCP Q Assign tab fields

Field	Description
Qset	Shows the assignment of Dscp values to a queue for each interface with a specific queue set. There are 64 instances of this class for each supported queue set.
Dscp	The DSCP value that maps to a queue in a queue set
Queue	A queue with which the traffic with a given DSCP value is associated.

Displaying DSCP mappings

To display DSCP mappings:

1 From the Device Manager menu bar, choose QoS/COPS > QoS Devices.

The QoSDevice dialog box opens with the Interface Queue tab displayed (Figure 69).

2 Click the DSCP mapping tab.

The DSCP mapping tab opens (Figure 77).

Figure 77 DSCP mapping tab

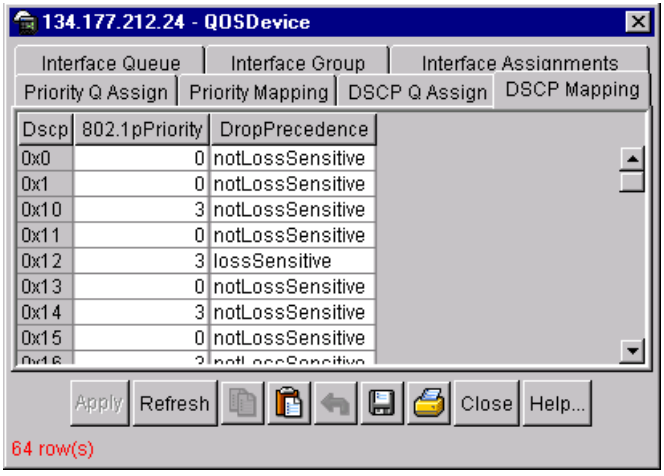


Table 61 describes the DSCP mapping tab fields.

Table 61 DSCP mapping tab fields

Field	Description
Dscp	Shows the DSCP value. This field is read-only.
802.1pPriority	A user priority value associated with the DSCP. To change a value, double-click in the cell and edit the value. The valid range is 0..7.
DropPrecedence	The drop precedence setting. The available settings are: • lossSensitive • notLossSensitive Traffic associated with lossSensitive drop precedence is generally given priority over traffic with notLossSensitive precedence during resource allocation. To change the setting, click in a cell and choose the setting.

Managing QoS rules

Displaying IP filters

To display IP filters:

➨ From the Device Manager menu bar, choose QoS/COPS > QoSRules.

The QoSRules dialog box opens with the IP filter tab displayed (Figure 78).

Figure 78 IP filter tab

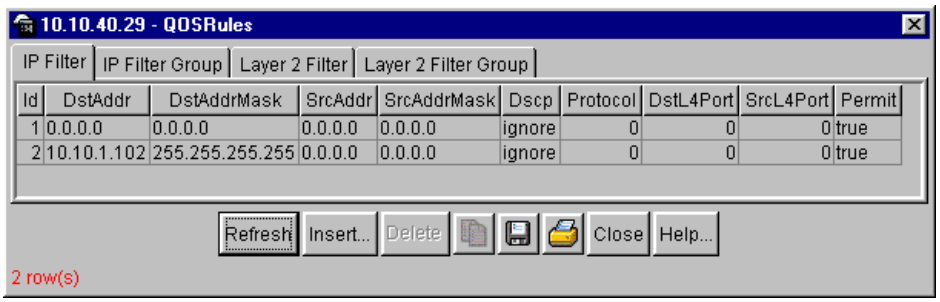


Table 62 describes the IP filter tab fields.

Table 62 IP filter tab fields

Field	Description
Id	The filter identifier.
DstAddr	The IP address that matches the packet's destination IP address.
DstAddrMask	The mask for matching the destination IP address.
SrcAddr	Specifies the source address to match against the packet's source IP address.
SrcAddrMask	The mask for matching the source IP address.
Dscp	The value that the DSCP in the packet must have and match the filter.
Protocol	The protocol that is matched against the packet's IP protocol field.
DstL4Port	The value the packet's layer 4 destination port must have and match this filter.

Table 62 IP filter tab fields (continued)

Field	Description
SrcL4Port	The value the packet's layer 4 source port must have and match this filter.
Permit	Specifies whether traffic with the above characteristics is considered a match (true) or not a match (false). If the frame matches the filter when this field is set to true, the matching process stops. True is the only value supported by Business Policy Switch.

Adding IP filters

To add an IP filter:

1. From the Device Manager menu bar, choose QoS/COPS > QoS Rules.

   The QoSRules dialog box opens with the IP filter tab displayed (Figure 78).

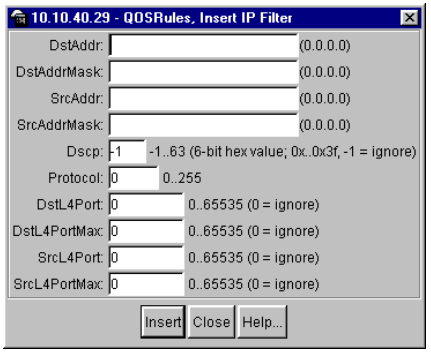
2. Click the IP filter tab.

   The IP filter tab opens (Figure 78).

3. Click Insert.

   The Insert IP filter dialog box opens (Figure 79).

Figure 79 Insert IP filter dialog box



4. Enter the information you want to use for this IP filter.
5. Click Insert.

Deleting IP filters

To delete an IP filter:

1 From the Device Manager menu bar, choose QoS/COPS > QoS Rules.

The QoSRules dialog box opens with the IP filter tab displayed (Figure 78).

2 Highlight the IP filter you want to delete.

3 Click Delete.

Note: You cannot delete an IP filter if it is referenced by a filter group.

Displaying IP filter groups

To display IP filter groups:

1 From the Device Manager menu bar, choose QoS/COPS > QoS Rules.

The QoSRules dialog box opens with the IP filter tab displayed (Figure 78).

2 Click the IP filter group tab.

The IP filter group tab opens (Figure 80).

Figure 80 IP filter group tab

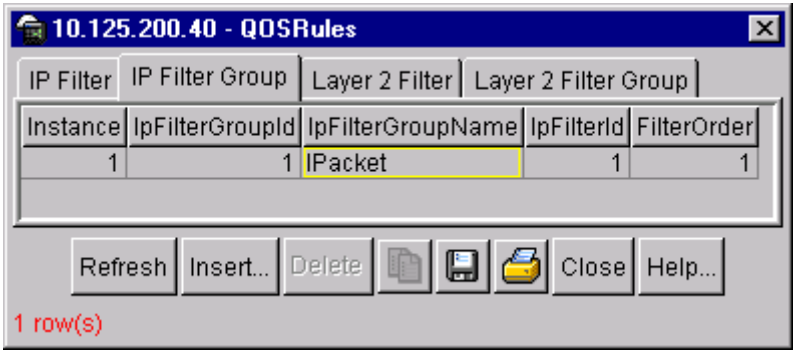


Table 63 describes the IP filter group tab fields.

Table 63 IP filter group tab fields

Field	Description
Instance	The unique identifier for this entry.
IpFilterGroupId	Specifies the identifier for an IP filter group.
IpFilterGroupName	Specifies the name for an IP filter group.
IpFilterId	Specifies the identifier for an IP filter.
FilterOrder	The evaluation order of filters in a group.

Adding IP filter groups

To add IP filter groups:

1 From the Device Manager menu bar, choose QoS/COPS > QoS Rules.

The QoSRules dialog box opens with the IP filter tab displayed (Figure 78).

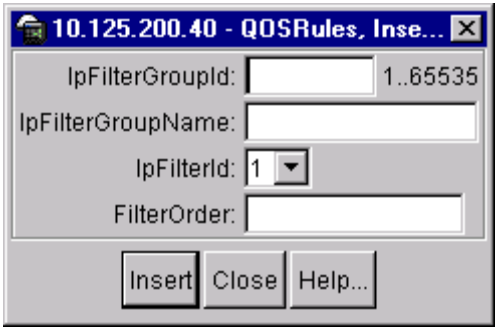
2 Click the IP filter group tab.

The IP filter group tab opens (Figure 80).

3 Click Insert.

The Insert IP filter group dialog box opens (Figure 81).

Figure 81 Insert IP filter group dialog box



4 Enter the information you want to use for this IP filter group.

5 Click Insert.

Deleting IP filter groups

To delete an IP filter groups:

1 From the Device Manager menu bar, choose QoS/COPS > QoS Rules.

The QoSRules dialog box opens with the IP filter tab displayed (Figure 78).

2 Click the IP filter group tab.

The IP filter group tab opens (Figure 80).

3 Highlight any table cell of the IP filter group you want to delete.

4 Click Delete.

Device Manager deletes the entire filter group.

Note: You cannot delete an IP filter group if it is the last entry for a given filter group and the group is referenced by a policy. You must first delete the policy.

Displaying Layer 2 filters

Device Manager lets you display Layer 2 filters.

To display Layer 2 filters:

1 From the Device Manager menu bar, choose QoS/COPS > QoS Rules.

The QoSRules dialog box opens with the IP filter tab displayed (Figure 78).

2 Click the Layer 2 filter tab.

The Layer 2 filter tab opens (Figure 82).

Figure 82 Layer 2 filter tab

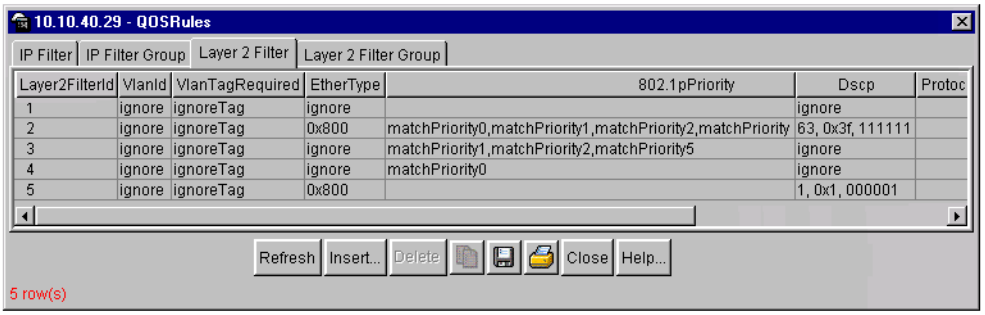


Table 64 describes the Layer 2 filter tab fields.

Table 64 Layer 2 filter tab fields

Field	Description
Layer2FilterId	The layer 2 filter identifier.
VlanId	The VLAN number. A value of -1 indicates that the VLAN ID is ignored.
VlanIdSet	Shows the VLANs referenced by the filter. The filter can reference up to 32 VLANs.
VlanTagRequired	Specifies whether or not to check the VLAN tagging.
EtherType	The etherType to match.
802.1pPriority	Specifies the 802.1 priority.
Dscp	The value that the DSCP in the packet must have and match the filter.
Protocol	The protocol that is matched against the packet's IP protocol field.
DstL4PortMin	The minimum value that the packet's layer 4 destination port number have and match the filter.
DstL4PortMax	The maximum value that the packet's layer 4 destination port number have and match the filter.
SrcL4PortMin	The minimum value that the packet's layer 4 source port number have and match the filter.
SrcL4PortMax	The maximum value that the packet's layer 4 source port number have and match the filter.

Adding Layer 2 filters

To add a Layer 2 filter:

1 From the Device Manager menu bar, choose QoS/COPS > QoS Rules.

The QoSRules dialog box opens with the IP filter tab displayed (Figure 78).

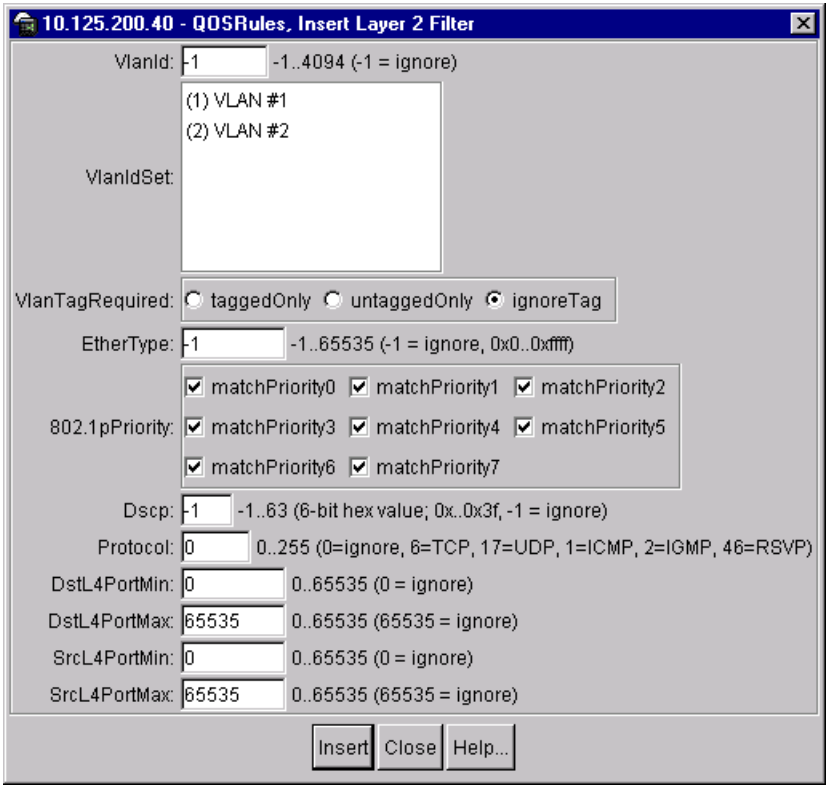
2 Click the Layer 2 filter tab.

The Layer 2 filter tab opens (Figure 82).

3 Click Insert.

The Insert Layer 2 filter dialog box opens (Figure 83).

Figure 83 Insert Layer 2 filter dialog box



4 Enter the information you want to use for this Layer 2 filter.

5 Click Insert.

Deleting Layer 2 filters

To delete a Layer 2 filter:

1 From the Device Manager menu bar, choose QoS/COPS > QoS Rules.

The QoSRules dialog box opens with the IP filter tab displayed (Figure 78).

2 Click the Layer 2 filter tab.

The Layer 2 filter tab opens (Figure 82).

3 Highlight the Layer 2 filter you want to delete.

4 Click Delete.

Note: You cannot delete an Layer 2 filter that is referenced in a filter group.

Displaying Layer 2 filter groups

To display Layer 2 filter groups:

1 From the Device Manager menu bar, choose QoS/COPS > QoS Rules.

The QoSRules dialog box opens with the IP filter tab displayed (Figure 78).

2 Click the Layer 2 filter tab.

The Layer 2 filter tab opens (Figure 82).

Figure 84 Layer 2 filter group tab

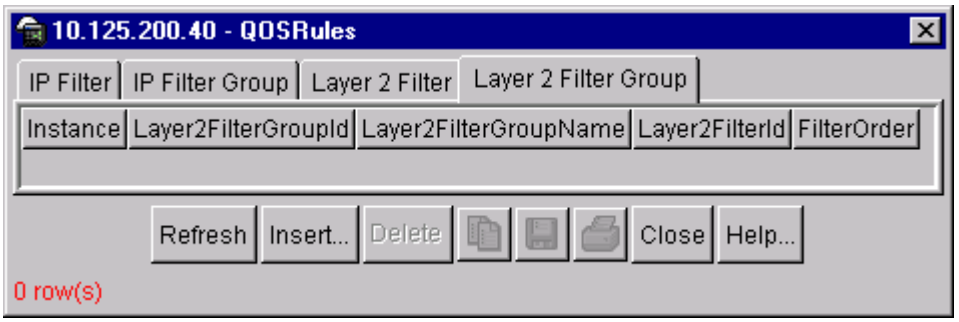


Table 65 describes the Layer 2 filter group tab fields.

Table 65 Layer 2 filter group tab fields

Field	Description
Instance	Specifies the unique identifier for this entry.
Layer2FilterGroupId	Specifies the identifier for a Layer 2 filter group.
Layer2FilterGroupName	Specifies the name for a Layer 2 filter group.
Layer2FilterId	Specifies the identifier for a Layer 2 filter.
Layer2FilterOrder	The evaluation order of filters in a group.

Adding Layer 2 filter groups

To add a Layer 2 filter group:

1 From the Device Manager menu bar, choose QoS/COPS > QoS Rules.

The QoSRules dialog box opens with the IP filter tab displayed (Figure 78).

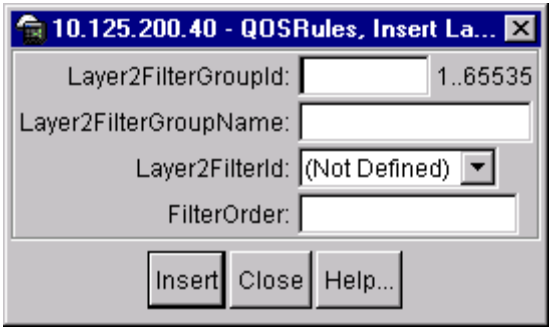
2 Click the Layer 2 filter group tab.

The Layer 2 filter group tab opens (Figure 84).

3 Click Insert.

The Insert Layer 2 filter group dialog box opens (Figure 85).

Figure 85 Insert Layer 2 filter group dialog box



4 Enter the information you want to use for this Layer 2 filter group.

5 Click Insert.

Deleting Layer 2 filter groups

To delete a Layer 2 filter group:

1 From the Device Manager menu bar, choose QoS/COPS > QoS Rules.

The QoSRules dialog box opens with the IP filter tab displayed (Figure 78).

2 Click the Layer 2 filter group tab.

The Layer 2 filter group tab opens (Figure 84).

3 Highlight the Layer 2 filter group you want to delete.

4 Click Delete.

Note: You cannot delete the last group entry in a Layer 2 filter group if it is referenced by a policy. You must first delete the policy.

Managing QoS actions, meters, shapers, and policies

Displaying QoS actions

To display a QoS action:

➨ From the Device Manager menu bar, choose QoS/COPS > QoS...

The QoS dialog box opens with the QoS action tab displayed (Figure 86).

Figure 86 QoS action tab

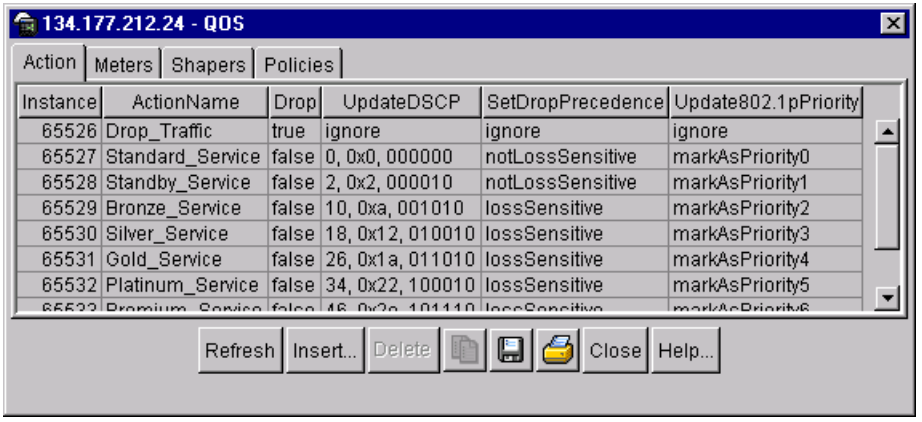


Table 66 describes the QoS action tab fields.

Table 66 QoS action tab fields

Field	Description
Instance	Specifies a unique identifier for the entry.
Action Name	Specifies a name for the entry.
Drop	Whether the frame being evaluated should be dropped (true) or not dropped (false).
UpdateDSCP	An integer that causes the value contained in the differentiated services field of an associated IP datagram to be updated with the value of the object.

Table 66 QoS action tab fields (continued)

Field	Description
SetDropPrecedence	Sets a precedence value. A value of 1 to 4 sets a low packet drop precedence. A value of 5 to 8 sets a high packet drop precedence. Other choices include: UseDefault, Ignore, and UseEgressMap.
UpdatePriority	A value that updates the value in the user priority field in the 802.1. The values range from 0 to 7, from lowest to highest priority. Other choices include: UseDefault, Ignore, and UseEgressMap.

Adding QoS actions

To add a QoS action:

1 From the Device Manager menu bar, choose QoS/COPS > QoS...

The QoS dialog box opens with the QoS action tab displayed (Figure 86).

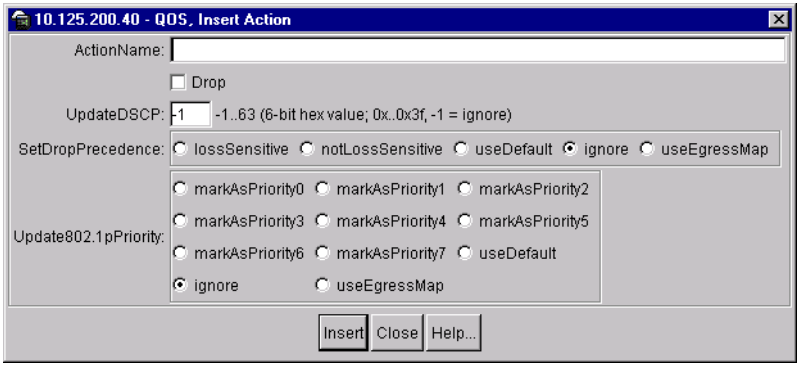
2 Click the QoS action tab.

The QoS action tab opens (Figure 86).

3 Click Insert.

The Insert QoS action dialog box opens (Figure 87).

Figure 87 Insert QoS action dialog box


10.125.200.40 - QOS, Insert Action
ActionName:
Drop
UpdateDSCP: -1 -1..63 (6-bit hex value; 0x..0x3f, -1 = ignore)
SetDropPrecedence: lossSensitive notLossSensitive useDefault ignore useEgressMap
Update802.1pPriority: markAsPriority0 markAsPriority1 markAsPriority2 markAsPriority3 markAsPriority4 markAsPriority5 markAsPriority6 markAsPriority7 useDefault ignore useEgressMap
Insert
Close
Help...

4 Enter the information and make the selections you want to use for this QoS action.

5 Click Insert.

Deleting QoS actions

To delete a QoS action:

1 From the Device Manager menu bar, choose QoS/COPS > QoS...

The QoS dialog box opens with the QoS action tab displayed (Figure 86).

2 Click the QoS action tab.

The QoS action tab opens (Figure 86).

3 Highlight the QoS action you want to delete.

4 Click Delete.

Note: You cannot delete a QoS action that is referenced by a meter entry. You must first delete the meter.

Displaying QoS meters

To display a QoS meter:

1 From the Device Manager menu bar, choose QoS/COPS > QoS...

The QoS dialog box opens with the QoS action tab displayed (Figure 86).

2 Click the QoS meters tab.

The QoS meters tab opens (Figure 88).

Figure 88 QoS meters tab

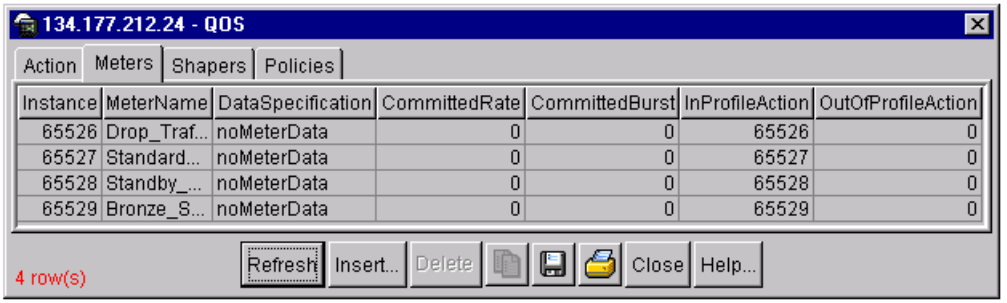


Table 67 describes the QoS meters tab fields.

Table 67 QoS meters tab fields

Field	Description
Instance	Specifies the unique identifier for this entry.
MeterName	Specifies a name for this entry.
DataSpecification	Specifies whether to meter the data or not. If you choose to not meter the data, the CommittedRate, CommittedBurst, and OutOfProfileAction fields are not applicable.
CommittedRate	Specifies the committed rate.
CommittedBurst	Specifies the committed burst.
InProfileAction	Specifies in profile action.
OutOfProfileAction	Specifies out of profile action.

Adding QoS meters

To add a QoS meter:

1 From the Device Manager menu bar, choose QoS/COPS > QoS...

The QoS dialog box opens with the QoS action tab displayed (Figure 86).

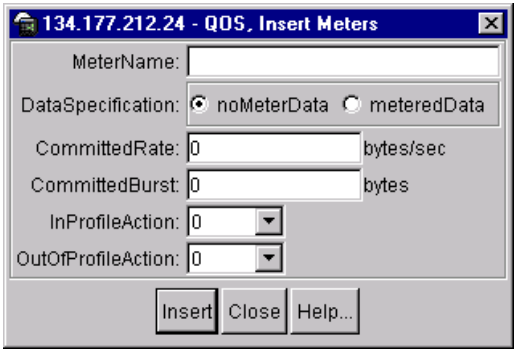
2 Click the QoS meters tab.

The QoS meters tab opens (Figure 88).

3 Click Insert.

The Insert QoS meters dialog box opens (Figure 89).

Figure 89 Insert QoS meters dialog box



4 Enter the information and make the selections you want to use for this QoS meters.

5 Click Insert.

Deleting QoS meters

To delete a QoS meter:

1 From the Device Manager menu bar, choose QoS/COPS > QoS...

The QoS dialog box opens with the QoS action tab displayed (Figure 86).

2 Click the QoS meters tab.

The QoS meters tab opens (Figure 88).

3 Highlight the QoS meters you want to delete.

4 Click Delete.

Note: You cannot delete a QoS meter that is referenced by a policy. You must first delete the policy.

Displaying QoS shapers

Note: You must be using either the BPS2000-1GT, BPS2000-2GT, or BPS2000-1GE MDA with the Business Policy Switch in order to implement the QoS shaping features.

For detailed information about traffic shaping, refer to *Using the Business Policy Switch 2000* and *Using Web-based Management for the Business Policy Switch 2000*.

To display QoS shapers:

1 From the Device Manager menu bar, choose QoS/COPS > QoS...

The QoS dialog box opens with the QoS action tab displayed (Figure 86).

2 Click the Shapers tab.

The QoS Shapers tab opens (Figure 88).

Figure 90 QoS Shapers tab

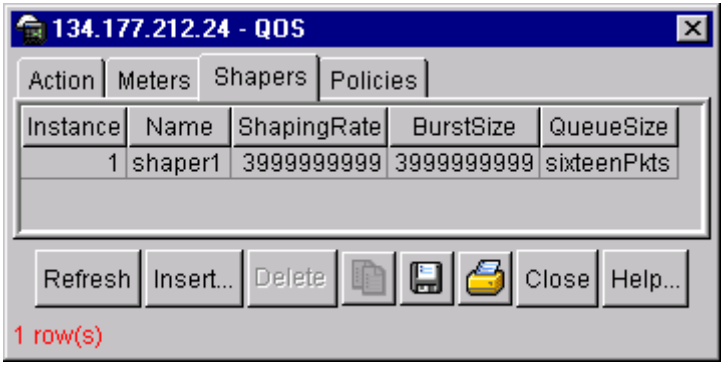


Table 67 describes the QoS Shapers tab fields.

Table 68 QoS Shapers tab fields

Field	Description
Instance	Specifies the unique identifier for this entry.
Name	Specifies the name for this entry.
ShapingRate	The maximum rate (in Kbps) at which traffic shaped using this shaper will be transmitted over a given duration. When you insert Shaper entries, you must enter a rate that is a multiple of 64 Kbps.
BurstSize	The maximum traffic burst size (in bytes) that can be transmitted without a shaping delay. The available values are: • 2047 • 4095 • 8191 • 16383 • 32767 • 65535
QueueSize	The number of packets that can exceed the traffic burst size and still be queued for transmission.

Adding QoS shapers

Note: You must be using either the BPS2000-1GT, BPS2000-2GT, or BPS2000-1GE MDA with the Business Policy Switch in order to implement the QoS shaping features.

For detailed information about traffic shaping, refer to *Using the Business Policy Switch 2000* and *Using Web-based Management for the Business Policy Switch 2000*.

To add a QoS shaper:

1 From the Device Manager menu bar, choose QoS/COPS > QoS.

The QoS dialog box opens with the QoS action tab displayed (Figure 86).

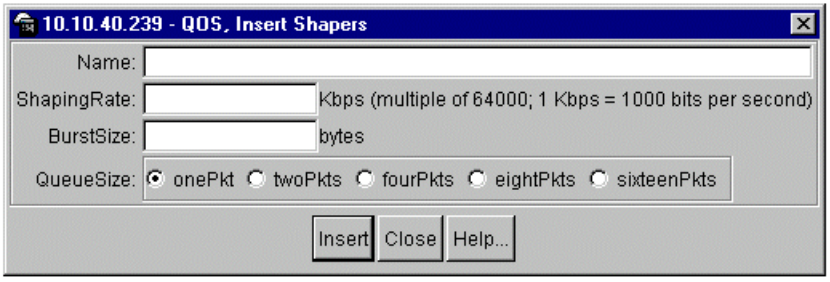
2 Click the QoS Shapers tab.

The QoS shapers tab opens (Figure 88).

3 Click Insert.

The Insert QoS Shapers dialog box opens (Figure 89).

Figure 91 Insert QoS shaper dialog box



4 Enter the information and make the selections you want to use for this QoS shaper.

5 Click Insert.

Deleting QoS shapers

Note: You must be using either the BPS2000-1GT, BPS2000-2GT, or BPS2000-1GE MDA with the Business Policy Switch in order to implement the QoS shaping features.

For detailed information about traffic shaping, refer to *Using the Business Policy Switch 2000* and *Using Web-based Management for the Business Policy Switch 2000*.

To delete a QoS shaper:

1 From the Device Manager menu bar, choose QoS/COPS > QoS.

The QoS dialog box opens with the QoS action tab displayed (Figure 86).

2 Click the QoS Shapers tab.

The QoS Shapers tab opens (Figure 88).

3 Highlight the QoS shaper you want to delete.

4 Click Delete.

Note: You cannot delete a QoS shaper that is referenced by a policy. You must first delete the policy.

Displaying QoS policies

To display QoS policies:

1 From the Device Manager menu bar, choose QoS/COPS > QoS...

The QoS dialog box opens with the QoS action tab displayed (Figure 86).

2 Click the QoS policies tab.

The QoS policies tab opens (Figure 92).

Figure 92 QoS policies tab

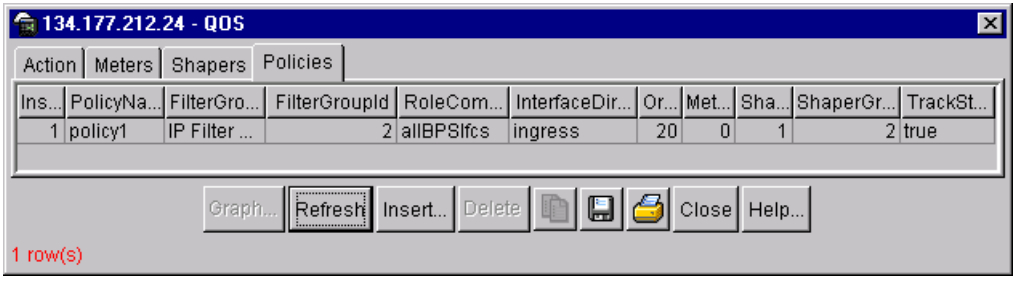


Table 69 describes the QoS policies tab fields.

Table 69 QoS policies tab fields

Field	Description
Instance	The unique identifier for this policy entry.
PolicyName	The name for this policy entry.
FilterGroupType	Specifies the type of filter group.
FilterGroupId	The filter group associated with a policy.

Table 69 QoS policies tab fields (continued)

Field	Description
RoleCombination	A tag that identifies the interfaces to which a policy specification applies.
InterfaceDirection	Specifies direction of packet flow at the specified interface. Business Policy Switch 2000 only supports ingress.
Order	The number used to determine the order of precedence for a policy specification.
Meter	Specifies the meter associated with a policy.
InProfileAction	The identifier of the in-profile action associated with the policy.
OutOfProfileAction	The identifier of the out-of-profile action associated with the policy.
Shaper	Specifies the shaper associated with a policy.
ShaperGroup	Specifies the shaper group associated with a policy.
TrackStatistics	Specifies whether statistics tracking is enabled or not.

Adding QoS policies

To add a QoS policy:

1 From the Device Manager menu bar, choose QoS/COPS > QoS...

The QoS dialog box opens with the QoS action tab displayed (Figure 86).

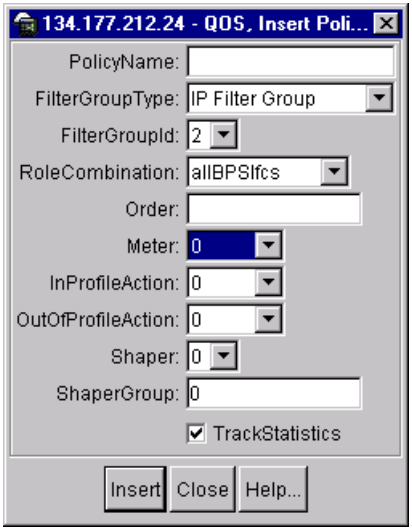
2 Click the QoS policies tab.

The QoS policies tab opens (Figure 92).

3 Click Insert.

The Insert QoS policies dialog box opens (Figure 93).

Figure 93 Insert QoS policies dialog box



4 Enter the information you want to use for this QoS policies.

5 Click Insert.

Deleting QoS policies

To delete a QoS policy:

1 From the Device Manager menu bar, choose QoS/COPS > QoS...

The QoS dialog box opens with the QoS action tab displayed (Figure 86).

2 Click the QoS policies tab.

The QoS policies tab opens (Figure 92).

3 Highlight the QoS policies you want to delete.

4 Click Delete.

Displaying QoS policy statistics

To display QoS policy statistics:

1 From the Device Manager menu bar, choose QoS/COPS > QoS.

The QoS dialog box opens with the QoS action tab displayed (Figure 86).

2 Highlight an entry in the QoS Policies tab. This activates the Graph button.

3 Click the Graph button.

The QoS policy statistics tab opens (Figure 94).

Figure 94 QoS policy statistics tab

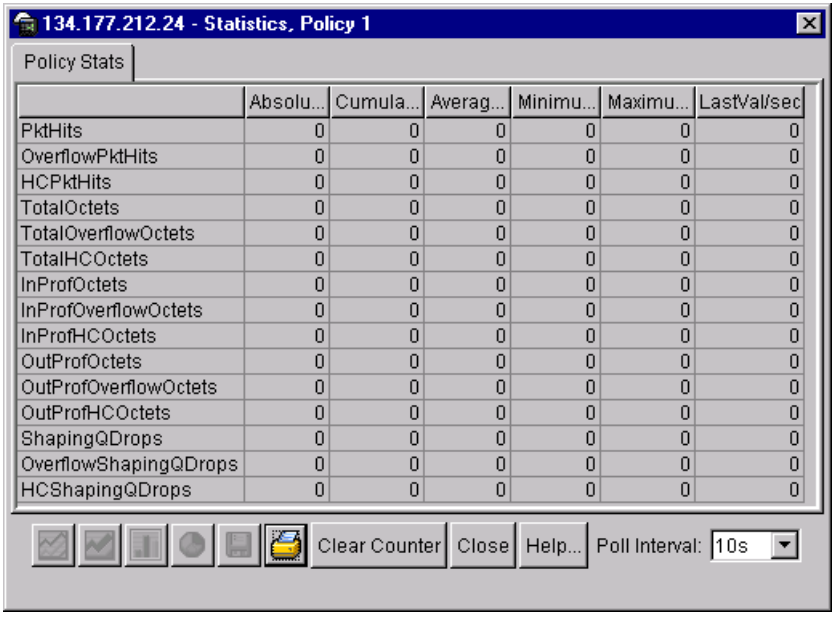

134.177.212.24 - Statistics, Policy 1
Policy Stats
Absolu...
Cumula...
Averag...
Minimu...
Maximu...
LastVal/sec
PktHits 0 0 0 0 0 0
OverflowPktHits 0 0 0 0 0 0
HCPktHits 0 0 0 0 0 0
TotalOctets 0 0 0 0 0 0
TotalOverflowOctets 0 0 0 0 0 0
TotalHCOctets 0 0 0 0 0 0
InProfOctets 0 0 0 0 0 0
InProfOverflowOctets 0 0 0 0 0 0
InProfHCOctets 0 0 0 0 0 0
OutProfOctets 0 0 0 0 0 0
OutProfOverflowOctets 0 0 0 0 0 0
OutProfHCOctets 0 0 0 0 0 0
ShapingQDrops 0 0 0 0 0 0
OverflowShapingQDrops 0 0 0 0 0 0
HCShapingQDrops 0 0 0 0 0 0
Clear Counter
Close
Help...
Poll Interval:
10s

Table 70 describes the QoS policy statistics tab fields.

Table 70 QoS policy statistics tab fields

Field	Description
PktHits	The packets selected for additional processing. The action taken is based on a match with a specified filter or threshold information.
OverflowPktHits	The number of times that the associated PkHits counter overflowed.
TotalOctets	The total number of octets associated with the packet hits for this policy.
TotalOverflowOctets	The total number of times that the associated TotalOctets counter overflowed.
InProfOctets	The total number of in-profile octets associated with packet hits for this policy.
InProfOverflowOctets	The total number of times that the associated InProfOctets counter overflowed.
OutProfOctets	The total number of out of profile octets associated with packet hits for this policy.
OutProfOverflowOctets	The total number of times the associated OutProfOctets counter overflowed.
ShapingQDrops	The number of packets dropped during shaping due to insufficient shaping queue resources.
OverflowSShapingQDrops	The number of times that the ShapingQDrops counter has overflowed.
HCShapingQDrops	A 64-bit counter that represents the combination of the OverflowSShapingQDrops and OverflowSShapingQDrops counters.

QoS agent

Displaying QoS agent configuration

To display QoS agent configuration:

➨ From the Device Manager menu bar, choose QoS/COPS > QoS Agent.

The QoSAgent dialog box opens with the configuration tab displayed (Figure 95).

Figure 95 configuration tab

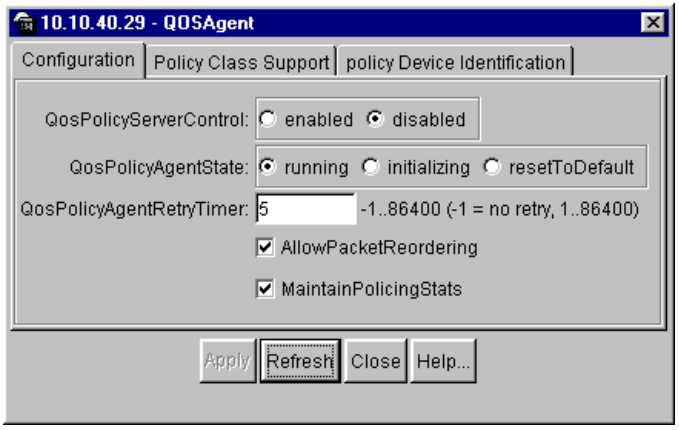


Table 71 describes the QoS Agent configuration tab fields.

Table 71 configuration tab fields

Field	Description
QosPolicyServerControl	Specifies whether policy server control is enabled or disabled.
QosPolicyAgentState	The current state of the policy agent.
QosPolicyAgentRetryTimer	The amount of time between each policy server retry.
AllowPacketReordering	Specifies whether packet reordering is acceptable.
MaintainPolicingStats	Specifies whether policy statistics should be maintained.

Displaying policy class support

To display policy class support:

1 From the Device Manager menu bar, choose QoS/COPS > QoS Agent.

The QoSAgent dialog box opens with the configuration tab displayed (Figure 95).

2 Click the Policy class support tab.

The policy class support tab opens (Figure 96).

Figure 96 Policy class support tab

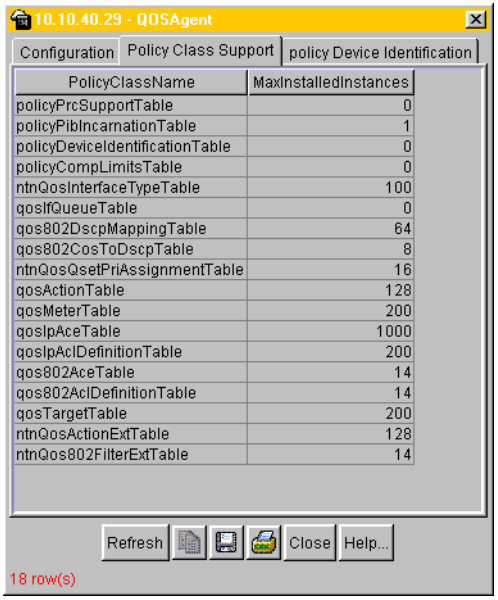


Table 72 describes the policy class support tab fields.

Table 72 policy class support tab fields

Field	Description
PolicyClassName	The name of the policy class.
MaximumInstalledInstances	The maximum number of installed instances of the policy class.

Displaying policy device identification

To display policy device identification data:

1 From the Device Manager menu bar, choose QoS/COPS > QoS Agent.

The QoSAgent dialog box opens with the configuration tab displayed (Figure 95).

2 Click the policy device identification tab.

The policy device identification tab opens (Figure 97).

Figure 97 Policy device identification tab

Table 73 describes the policy device identification tab fields.

Table 73 policy device identification tab fields

Field	Description
Descr	A description of the policy device.
MaxMsg	The maximum message size in bytes that the device can support.

COPS overview

COPS is a comprehensive network management application for policy-based network traffic control. The policy server distributes policies to edge devices and border routers.COPS is used to communicate with edge devices on the network. Some of the benefits of the COPS protocol are:

- It uses a client/server model for communication between the policy server and the policy clients.
- It uses TCP for messaging, reducing the resources it requires.
- The policy server can send configuration information to the policy client, as well as removing unneeded configuration information.

Displaying COPS capabilities

To display COPS capabilities:

➡ From the Device Manager menu bar, choose QoS/COPS > QoS COPS.

The COPS dialog box opens with the capabilities tab displayed (Figure 98).

Figure 98 capabilities

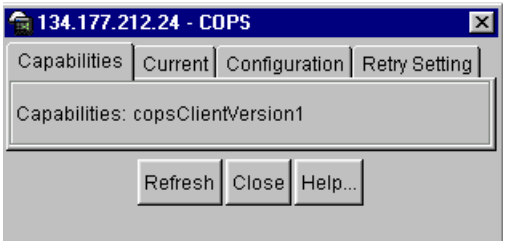


Table 74 describes the Capabilities tab fields.

Table 74 Capabilities tab fields

Field	Description
Capabilities	A list of COPS protocols supported by Business Policy Switch 2000.

Displaying COPS current service configuration

To display current service configuration data:

1 From the Device Manager menu bar, choose QoS/COPS > COPS.

The COPS dialog box opens with the capabilities tab displayed (Figure 98).

2 Click the current tab.

The current tab opens (Figure 99).

Figure 99 Current

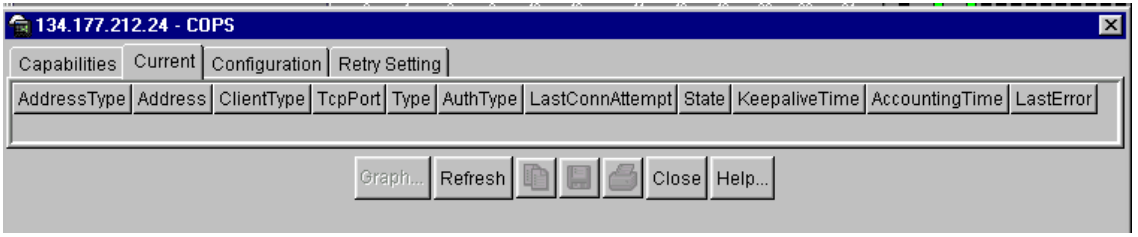


Table 75 describes the current tab fields.

Table 75 Current tab fields

Field	Description
AddressType	The type of address in the copsClientServerAddress.
Address	The IPv4, IPv6, or DNS address of a COPS server.
ClientType	The protocol client type for an entry.
TcpPort	The TCP port number on the COPS server that the client is connected to.
Type	The source of COPS server information.
AuthType	The security mode being used between the client and the COPS server.
LastConnAttempt	The timestamp of the last time that the client attempted to connect to the COPS server.
State	The operational state of a connection between a client and the COPS server.
KeepaliveTime	The value of the keepalive timeout, in centiseconds, that is currently in use by a client. The COPS server specifies this value in the Client-Accept operation.
AccountingTime	The value of the COPS protocol Accounting timeout, in centiseconds, that is currently in use by a client. The COPS server specifies this value in the Client-Accept operation.
LastError	The code contained in the last protocol Error Object received from the COPS server.

Displaying COPS local configuration

To display COPS configuration data:

1 From the Device Manager menu bar, choose QoS/COPS > COPS.

The COPS dialog box opens with the capabilities tab displayed.

2 Click the configuration tab.

The configuration tab opens (Figure 100).

Figure 100 Configuration

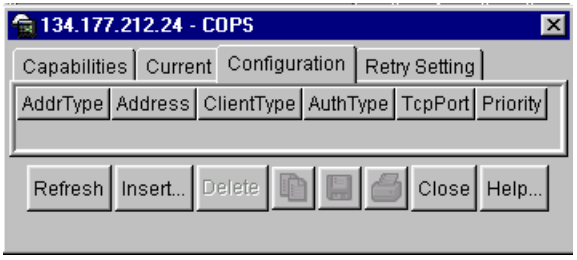


Table 76 describes the configuration tab fields.

Table 76 Configuration tab fields

Field	Description
AddrType	The type of address.
Address	The address identifier.
ClientType	The type of client
AuthType	The security mode being used between the client and the COPS server.
TcpPort	The TCP port number on the COPS server that the client is connected to.
Priority	The level of priority.

Adding COPS local configuration data

To add COPS local configuration data:

1 From the Device Manager menu bar, choose QoS/COPS > COPS.

The COPS dialog box opens with the capabilities tab displayed.

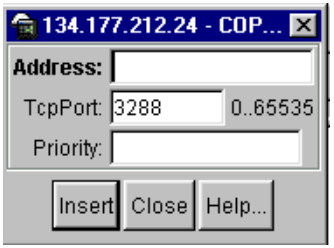
2 Click the configuration tab.

The configuration tab opens (Figure 100).

3 Click Insert.

The Insert COPS configuration dialog box opens (Figure 101).

Figure 101 Insert COPS configuration dialog box



4 Enter the information you want to use for this COPS configuration.

5 Click Insert.

Deleting COPS local configuration data

To delete COPS local configuration data:

1 From the Device Manager menu bar, choose QoS/COPS > COPS.

The COPS dialog box opens with the capabilities tab displayed.

2 Click the configuration tab.

The configuration tab opens (Figure 100).

3 Highlight the COPS configuration you want to delete.

4 Click Delete.

Displaying COPS retry setting

To display COPS retry setting:

1 From the Device Manager menu bar, choose QoS/COPS > COPS.

The COPS dialog box opens with the capabilities tab displayed.

2 Click the retry setting tab.

The retry setting tab opens (Figure 102).

Figure 102 Retry Setting

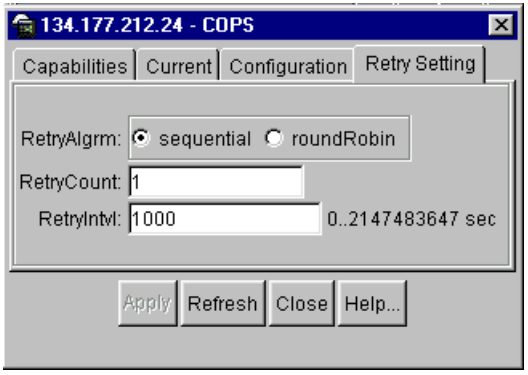


Table 77 describes the tab fields.

Table 77 COPS Retry setting tab fields

Field	Description
RetryAlgrm	The type of algorithm.
RetryCount	The number of retry attempts.
RetryIntvl	The retry interval in seconds.

To make changes to the information in the Retry setting tab:

1 Make the changes you want in the Retry setting tab.

2 Click on the Apply button to confirm the changes.

Displaying COPS statistics

To display COPS statistics:

1 In the Current tab, highlight an entry and click on the Graph button.

The COPS statistics dialog box opens.

2 Click the COPS statistics tab.

The COPS statistics tab is active (Figure 103).

Figure 103 COPS statistics

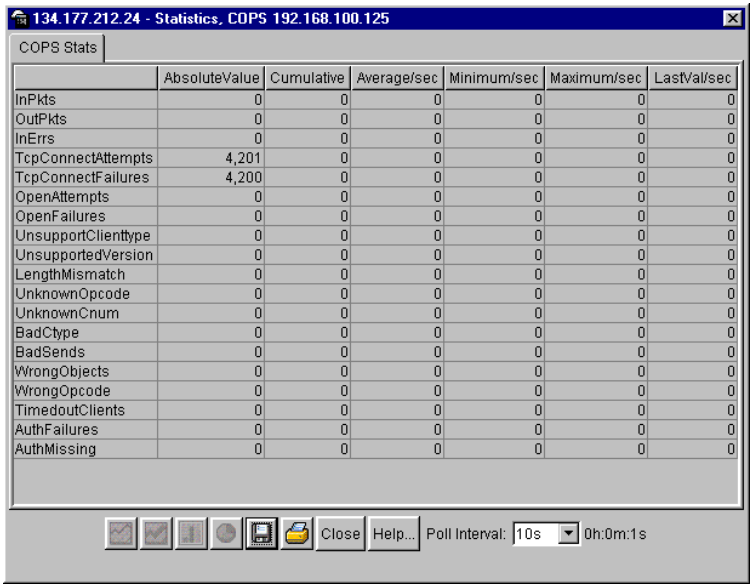

134.177.212.24 - Statistics, COPS 192.168.100.125
COPS Stats
AbsoluteValue Cumulative Average/sec Minimum/sec Maximum/sec LastVal/sec
InPkts 0 0 0 0 0 0
OutPkts 0 0 0 0 0 0
InErrs 0 0 0 0 0 0
TcpConnectAttempts 4,201 0 0 0 0 0
TcpConnectFailures 4,200 0 0 0 0 0
OpenAttempts 0 0 0 0 0 0
OpenFailures 0 0 0 0 0 0
UnsupportClienttype 0 0 0 0 0 0
UnsupportedVersion 0 0 0 0 0 0
LengthMismatch 0 0 0 0 0 0
UnknownOpcode 0 0 0 0 0 0
UnknownCnum 0 0 0 0 0 0
BadCtype 0 0 0 0 0 0
BadSends 0 0 0 0 0 0
WrongObjects 0 0 0 0 0 0
WrongOpcode 0 0 0 0 0 0
TimedoutClients 0 0 0 0 0 0
AuthFailures 0 0 0 0 0 0
AuthMissing 0 0 0 0 0 0
Close
Help...
Poll Interval:
10s
0h:0m:1s

Table 78 describes the COPS statistics tab fields.

Table 78 COPS statistics tab fields

Field	Description
InPkts	The total number of COPS messages received for this client type.
OutPkts	The total number of COPS messages sent for this client type.
InErrs	The total number of COPS messages received for this client type that contained an error in syntax.
TcpConnectAttempts	The total number of TCP connections attempted to this COPS server for this client type.
TcpConnectFailures	The total number of TCP connections to this COPS server for this client type that failed.
OpenAttempts	The total number of attempts to perform a COPS Client-Open to this COPS server for this client type.
OpenFailures	The total number of failed attempts to perform a COPS Client -Open to this COPS server for this client type.
UnsupportClientType	The total number of COPS messages received from this COPS server containing unsupported client types.
UnsupportedVersion	The total number of COPS messages received from this COPS server containing an unsupported protocol version.
LengthMismatch	The total number of COPS messages received from this COPS server for this client type where the COPS protocol message length did not match the actual message length.
UnknownOpcode	The total number of COPS messages received from this COPS server for this client type which contained an unrecognized COPS protocol op code.
UnknownCnum	The total number of COPS messages received from this COPS server for this client type that contained an unrecognized COPS object C-Num.
BadCtype	The total number of COPS messages received from this COPS server for this client type which contained a COPS protocol object C-type that was not defined for the C-Nums known by the COPS client.
BadSends	The total number of COPS messages the client attempted to send to the COPS server for which a transit error occurred.
WrongObjects	The total number of COPS messages received from this COPS server for this client type which contained a set of COPS protocol objects that are not permitted.
WrongOpcode	The total number of COPS messages received from this COPS server for this client type containing a COPS protocol op code that should not be sent to a COPS client.

Table 78 COPS statistics tab fields (continued)

Field	Description
TimeoutClients	The total number of times this client has been shut down for this client type by COPS servers that detected a COPS protocol keepalive timeout.
AuthFailures	The total number of COPS messages received from this COPS server for this client type which could not be authenticated with the authentication method used by the client.
AuthMissing	The total number of COPS messages received from this COPS server for this client type which did not contain required authentication information.

Chapter 8
Setting up bridging

The Bridge parameters allow you to view MAC address table for a Business Policy Switch.

This chapter describes the bridge information available in Device Manager on the following tab:

- Base tab (next)

Base tab

The MAC address used by the bridge must be referred to in a unique fashion; moreover, it should be the smallest MAC address (numerically) of all ports that belong to the bridge. However, it is only required to be unique when integrated with `dot1dStpPriority`. A unique `BridgeIdentifier` is formed that is used in the Spanning Tree Protocol.

To view the Base tab:

➨ From the Device Manager menu bar, select Edit > Bridge.

The Bridge dialog box opens with the Base tab displayed (Figure 104).

Figure 104 Base tab

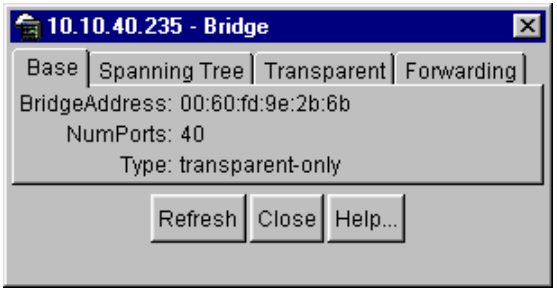


Table 79 describes the Base tab fields.

Table 79 Base tab fields

Field	Description
BridgeAddress	MAC address of the bridge when it is referred to in a unique fashion. This address should be the smallest MAC address of all ports that belong to the bridge. However, it is has to be unique. When concatenated with dot1dStpPriority, a unique bridge ID is formed that is then used in the Spanning Tree Protocol.
NumPorts	Number of ports controlled by the bridging entity.
Type	Indicates the type of bridging this bridge can perform. If the bridge is actually performing a certain type of bridging, this fact will be indicated by entries in the port table for the given type.

Spanning Tree tab

The Spanning Tree tab displays the version of the spanning tree protocol currently running. If future versions of the IEEE spanning tree protocol are released that are incompatible with the current version, a new value will be defined.

To view the Spanning Tree tab:

1 From the Device Manager menu bar, choose Edit > Bridge.

The Bridge dialog box opens, with the Base tab displayed.

2 Click the Spanning Tree tab.

The Spanning Tree tab opens (Figure 105).

Figure 105 Spanning Tree tab

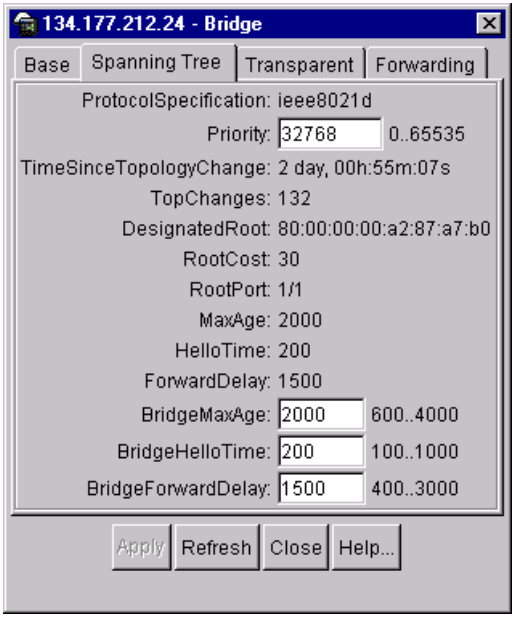


Table 80 describes the Spanning Tree tab fields.

Table 80 Spanning Tree tab fields

Field	Description
ProtocolSpecification	Version of the spanning tree protocol being run. Values include: • decLb100: Indicates the DEC LANbridge 100 spanning tree protocol. • ieee8021d: IEEE 802.1d implementations will return this entry. When future versions of the IEEE spanning tree protocol are released that are incompatible with the current version, a new value will be defined.
Priority	Value of the writable portion of the bridge ID. That is, the first two octets of the (8-octet long) bridge ID. The last six octets of the bridge ID are given by the value of BridgeAddress.
TimeSinceTopologyChange	Time (in hundredths of a second) since the last time a topology change was detected by the bridge entity.

Table 80 Spanning Tree tab fields (continued)

Field	Description
TopChanges	Number of topology changes detected by this bridge since the management entity was reset or initialized.
DesignatedRoot	Bridge ID of the root of the spanning tree as determined by the Spanning Tree Protocol. This is executed by the node. This value is used as the Root ID parameter in all configuration bridge PDUs originated by the node.
RootCost	Cost of the path to the root as seen from this bridge.
RootPort	Port number of the port that offers the lowest cost path from this bridge to the root bridge.
MaxAge	Maximum age of Spanning Tree Protocol information learned from the network on any port before it is discarded, in units of hundredths of a second. This is the actual value that this bridge is currently using.
HelloTime	Time between the transmission of Configuration bridge PDUs by the node on any port when it is the root of the spanning tree (in units of hundredths of a second). This is the actual value that the bridge is currently using.
ForwardDelay	Value (in hundredths of a second) that controls how fast a port changes its spanning state when moving towards the Forwarding state. The value determines how long the port stays in each of the Listening and Learning states, that precede the Forwarding state. The value is also used when a topology change has been detected and is underway. This ages all dynamic entries in the Forwarding Database. **Note**: This value is the one that this bridge is currently using, in contrast to dot1dStpBridge ForwardDelay which is the value that this bridge and all others would start using if/when this bridge were to become the root.]
BridgeMaxAge	Value that all bridges use for the maximum age of a bridge when it is acting as the root. **Note**: 802.1D-1990 specifies that the range is related to the value of BridgeHelloTime. The granularity of this timer is specified by 802.1D-1990 to be 1 second. A badValue error may be returned if the value set is not a whole number.

Table 80 Spanning Tree tab fields (continued)

Field	Description
BridgeHelloTime	Value that the bridge uses for HelloTime when the bridge is acting as the root. The granularity of this timer is specified by 802.1D- 1990 to be one second. An agent may return a badValue error if a set is attempted to a value that is not a whole number of seconds.
TimeSinceTopologogyChange	Value that all bridges use for ForwardDelay when this bridge is acting as the root. Note: 802.1D-1990 specifies that the range for this parameter is related to the value of dot1dStpBridgeMaxAge. The granularity of this timer is specified by 802.1D-1990 to be one second. An agent may return a badValue error if a set is attempted to a value that is not a whole number of seconds.

Transparent tab

The Transparent tab contains information about a specific unicast MAC address, which has some forwarding information for the bridge.

To view the Transparent tab:

1 From the Device Manager menu bar, choose Edit > Bridge.

The Bridge dialog box opens, with the Base tab displayed.

2 Click the Transparent tab.

The Transparent tab opens (Figure 106).

Figure 106 Transparent tab

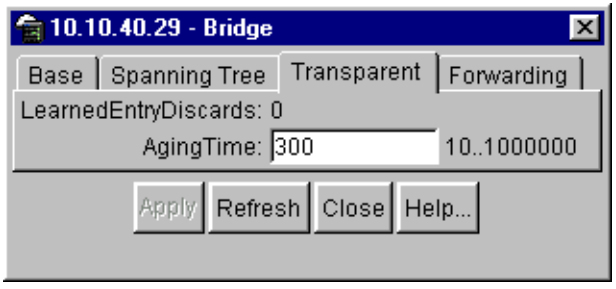


Table 81 describes the Transparent tab items.

Table 81 Transparent tab items

Item	Description
LearnedEntryDiscard	Number of Forwarding Database entries learned that have been discarded due to a lack of space in the Forwarding Database. If this counter is increasing, it indicates that the Forwarding Database is becoming full regularly. This condition will effect the performance of the subnetwork. If the counter has a significant value and is not presently increasing, it indicates that the problem has been occurring but is not persistent.
AgingTime	Time-out period in seconds for aging out dynamically learned forwarding information. **Note**: The 802.1D-1990 specification recommends a default of 300 seconds.

Forwarding tab

The Forwarding tab displays the current state of the port, as defined by application of the Spanning Tree Protocol. This state controls what action a port takes on reception of a frame. If the bridge detects a port that is malfunctioning, it places the port into the "broken" state. For ports that are disabled, the value is "disabled."

To view the Forwarding tab:

1 From the Device Manager menu bar, choose Edit > Bridge.

The Bridge dialog box opens, with the Base tab displayed.

2 Click the Forwarding tab.

The Forwarding tab opens (Figure 107).

Figure 107 Forwarding tab

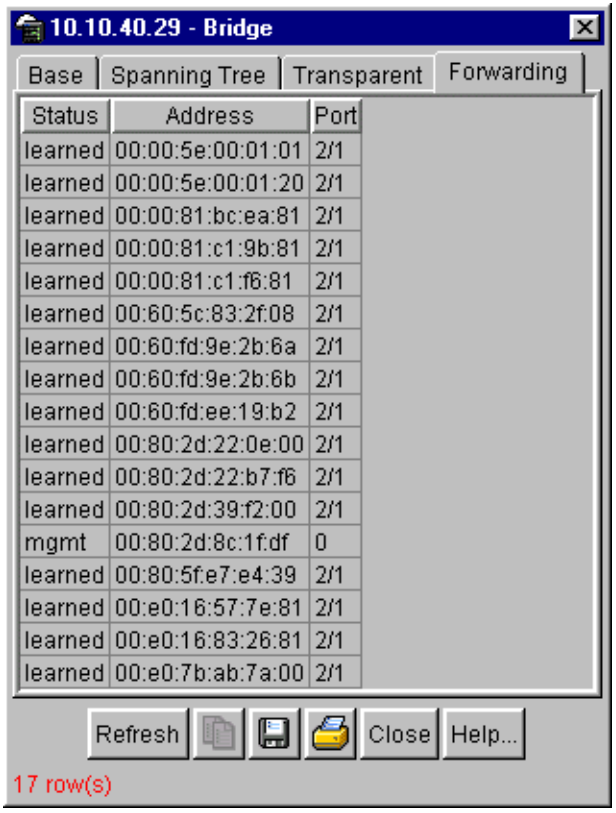


Table 82 describes the Forwarding tab fields.

Table 82 Forwarding tab fields

Field	Description
Status	The values of this fields include: • invalid: Entry is no longer valid, but has not been removed from the table. • learned: Value of the corresponding instance of dot1dTpFdbPort was learned and is being used. • self: Value of the corresponding instance of dot1dTpFdbAddress represents an address of the bridge. The corresponding instance of dot1dTpFdbPort indicates that a specific port on the bridge has this address. • mgmt(5): Value of the corresponding instance of dot1dTpFdbAddress is also the value of an existing instance of dot1dStaticAddress. • other: none of the preceding. This would include where some other MIB object (not the corresponding instance of dot1dTpFdbPort or an entry in the dot1dStaticTable) is being used to determine if a frames addressed to the value of dot1dTpFdbAddress are being forwarded.
Address	A unicast MAC address for which the bridge has forwarding or filtering information.
Port	Either the value “0” or the port number on a frame has been seen. The source address must be equal to the value of the corresponding instance of dot1dTpFdbAddress A value of “0” indicates that the port number has not been learned, so the bridge does have the forwarding/filtering information for this address (located in the dot1dStaticTable). You should assign the port value to this object whenever it is learned even for addresses for which the corresponding value of dot1dTpFdbStatus is not learned(3).

Chapter 9
Troubleshooting Device Manager

This chapter describes diagnostic information available in Device Manager on the following tabs:

- Topology tab (this page)
- Topology Table tab (page 206)

Topology tab

To view topology information:

➨ From the Device Manager menu bar, select Edit > Diagnostics.

The Diagnostics dialog box opens with the Topology tab displayed (Figure 108).

Figure 108 Diagnostics dialog box — Topology tab

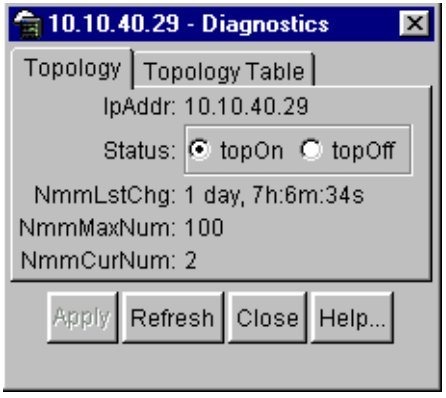


Table 83 describes the Topology tab items.

Table 83 Topology tab items

Items	Description
IpAddr	The IP address of the device.
Status	Whether Nortel Networks topology is on (topOn) or off (topOff) for the device. The default value is topOn.
NmmLstChg	The value of sysUpTime the last time an entry in the network management MIB (NMM) topology table was added, deleted, or modified. If the table has not changed since the last cold or warm start of the agent.
NmmMaxNum	The maximum number of entries in the NMM topology table.
NmmCurNum	The current number of entries in the NMM topology table.

Topology Table tab

To view more topology information:

1 From the Device Manager menu bar, choose Edit > Diagnostics.

The Diagnostics dialog box opens with the Topology tab displayed (Figure 108).

2 Click the Topology Table tab.

The Topology Table tab opens (Figure 109).

Figure 109 Diagnostics dialog box — Topology Table tab

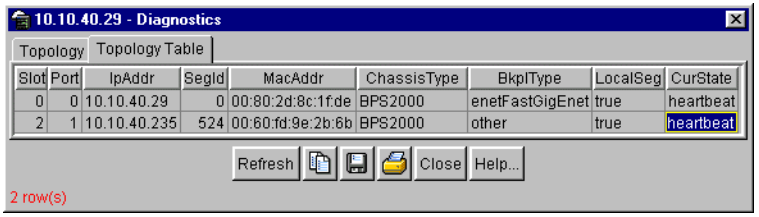


Table 84 describes the Topology Table tab fields.

Table 84 Topology Table tab fields

Field	Description
Slot	The slot number in the chassis in which the topology message was received.
Port	The port on which the topology message was received.
IpAddr	The IP address of the sender of the topology message.
SegId	The segment identifier of the segment from which the remote agent sent the topology message. This value is extracted from the message.
MacAddr	The MAC address of the sender of the topology message.
ChassisType	The chassis type of the device that sent the topology message.
BkplType	The backplane type of the device that sent the topology message.
LocalSeg	Indicates if the sender of the topology message is on the same Ethernet segment as the reporting agent.
CurState	The current state of the sender of the topology message. The choices are: • topChanged —Topology information has recently changed. • heartbeat —Topology information is unchanged. • new — The sending agent is in a new state.

Chapter 10
RMON

The Remote Network Monitoring (RMON) MIB is an interface between the RMON agent on a Business Policy Switch 2000 and an RMON management application, such as the Device Manager.

It defines objects that are suitable for the management of any type of network, but some groups are targeted for Ethernet networks in particular.

The RMON agent continuously collects statistics and proactively monitors switch performance. You can view this data through the Device Manager.

RMON has three major functions:

- Creating and displaying alarms for user-defined events
- Gathering cumulative statistics for Ethernet interfaces
- Tracking a history of statistics for Ethernet interfaces

Working with RMON information

You can view RMON information by looking at the Graph information associated with the port or chassis.

Viewing statistics

Device Manager gathers Ethernet statistics that you can have graphed in a variety of formats, or you can save them to a file and export the statistics to an outside presentation or graphing application.

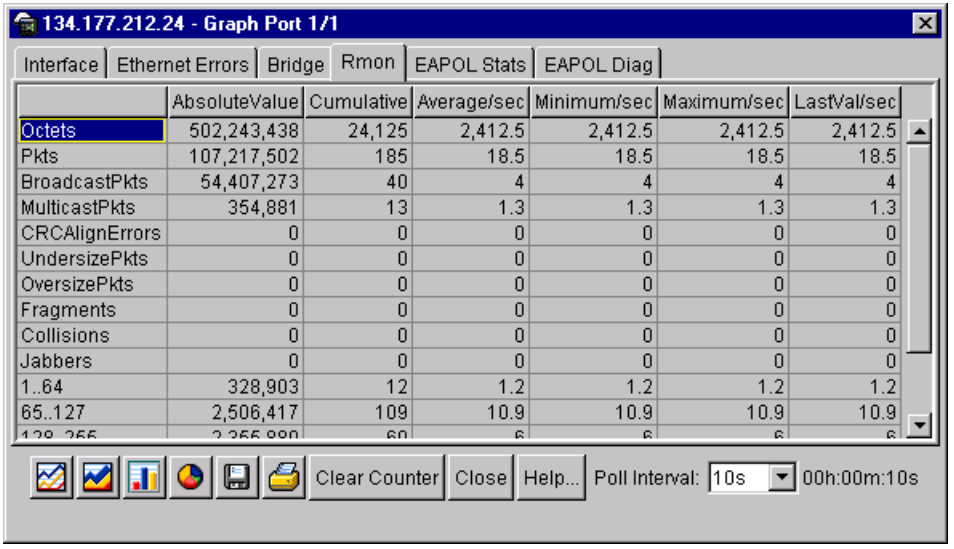
To view RMON Ethernet statistics:

1. Select an object (port or chassis).
2. Do one of the following:
   - From the shortcut menu, choose Graph.
   - From the Device Manager main menu, choose Graph > Port.
   - On the toolbar, click Graph button.

   The graph Port dialog box opens displaying the Interface tab (Figure 110).
3. Click the RMON tab.

   The RMON tab opens and displays the Ethernet statistics (Figure 110).

Figure 110 Port dialog box — RMON tab



For descriptions of the RMON tab fields, refer to Table 42 on page 111. For descriptions of the statistics columns, refer to Table 12 on page 44.

Viewing history

Ethernet history records periodic statistical samples from a network. A sample is called a history and is gathered in time intervals referred to as “buckets.” Histories establish a time-dependent method for gathering RMON statistics on a port. The default values for history are:

- Buckets are gathered at 30-minute intervals.
- Number of buckets gathered is 50.

Both the time interval and the number of buckets is configurable. However, when the last bucket is reached, bucket 1 is dumped and “recycled” to hold a new bucket of statistics. Then bucket 2 is dumped, and so forth.

To view RMON history:

1 From the Device Manager main menu, choose RMON > Control > History

1 Select an RMON entry.

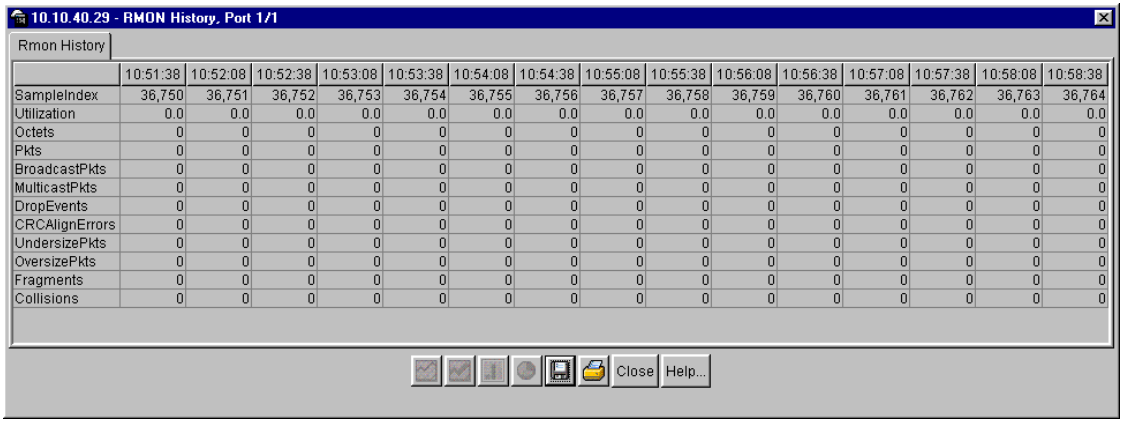
2 On the toolbar, click Graph.

The RMON graph Port dialog box opens displaying the Interface tab.

3 Click the RMON tab.

The RMON tab opens (Figure 111).

Figure 111 Port dialog box — RMON History tab



	10:51:38	10:52:08	10:52:38	10:53:08	10:53:38	10:54:08	10:54:38	10:55:08	10:55:38	10:56:08	10:56:38	10:57:08	10:57:38	10:58:08	10:58:38
SampleIndex	36,750	36,751	36,752	36,753	36,754	36,755	36,756	36,757	36,758	36,759	36,760	36,761	36,762	36,763	36,764
Utilization	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Octets	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Pkts	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
BroadcastPkts	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MulticastPkts	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DropEvents	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CRCAlignErrors	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
UndersizePkts	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
OversizePkts	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Fragments	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Collisions	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Creating a history

You can use RMON to collect statistics at intervals. For example, if you want RMON statistics to be gathered over the weekend, you will want enough buckets to cover two days. To do this, set the history to gather one bucket each hour, thus covering a 48-hour period. After you set history characteristics, you cannot modify them; you must delete the history and create another one.

To establish a history for a port and set the bucket interval:

1 From the Device Manager main menu, choose RMON > Control.

The RMONControl dialog box opens with the History tab displayed (Figure 112).

Figure 112 History tab

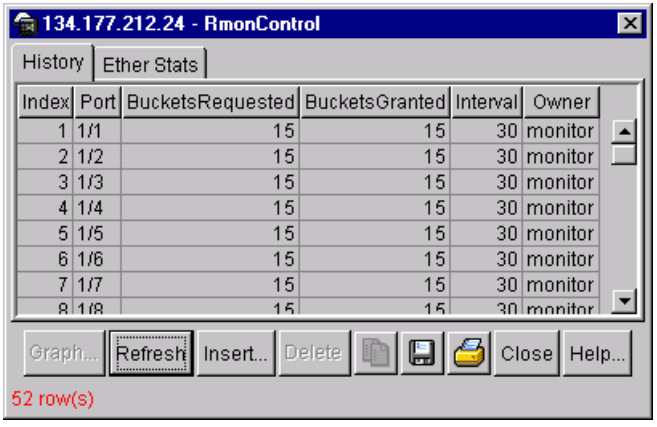
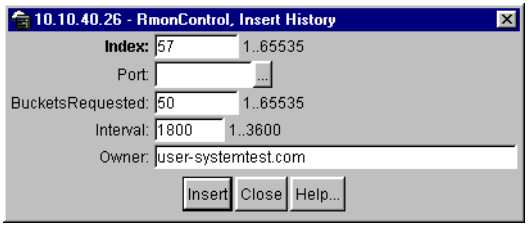


Table 85 describes the History fields.

2 Select an index and then click Insert.

The RmonControl, Insert History dialog box opens (Figure 113).

Figure 113 RMONControl, Insert History dialog box



3 Select the port from the port list or type the port number.

4 Set the number of buckets.

The default is 50.

5 Set the interval.

The default is 1800 seconds.

6 Type the owner, the network management system that created this entry.

7 Click Insert.

Table 85 describes the History tab of the RmonControl dialog box.

Table 85 History tab fields

Field	Description
Index	A unique value assigned to each interface. An index identifies an entry in a table.
Port	Any Ethernet interface on the device.
BucketsRequested	The requested number of discrete time intervals over which data is to be saved in the part of the media-specific table associated with this entry.
BucketsGranted	The number of discrete sampling intervals over which data is saved in the part of the media-specific table associated with this entry. There are instances when the actual number of buckets associated with this entry is less than the value of this object. In this case, at the end of each sampling interval, a new bucket is added to the media-specific table.

Table 85 History tab fields (continued)

Field	Description
Interval	The interval in seconds over which the data is sampled for each bucket in the part of the media-specific table associated with this entry. You can set this interval to any number of seconds between 1 and 3600 (1 hour). Because the counters in a bucket may overflow at their maximum value with no indication, note the possibility of overflow in any of the associated counters. It is important to consider the minimum time in which any counter could overflow on a particular media type and set the historyControlInterval object to a value less than this interval. This is typically most important for the 'octets' counter in any media-specific table. For example, on an Ethernet network, the etherHistoryOctets counter could overflow in about one hour at the Ethernet's maximum utilization.
Owner	The network management system that created this entry.

Disabling history

To disable RMON history on a port:

1 From the Device Manager main menu, choose RMON > Control.

The RMONControl dialog box opens with the History tab displayed (Figure 112).

2 Highlight the row that contains the port ID you want to delete.

3 Click Delete.

The entry is removed from the table.

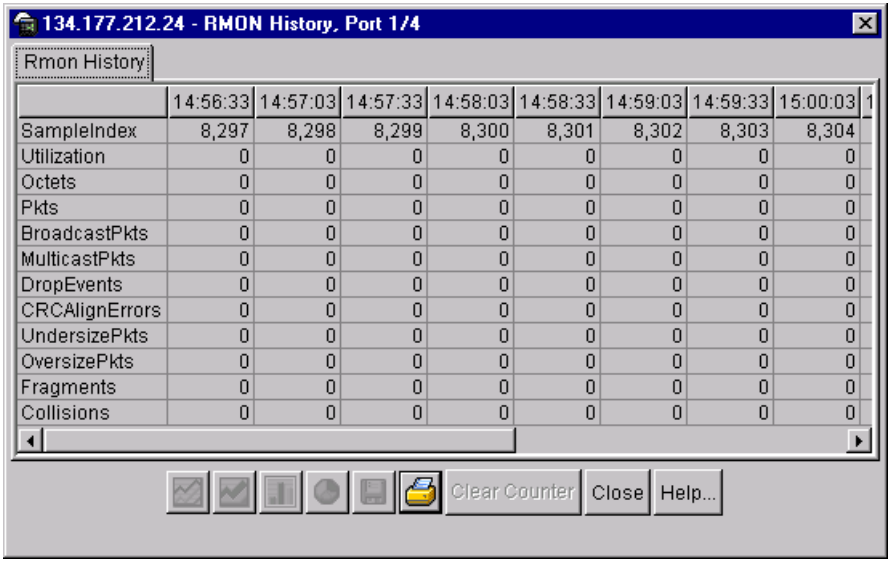
Viewing RMON history statistics

To display Rmon history statistics:

➨ In the Rmon history tab, highlight an entry and click on the Graph button.

The Rmon history statistics dialog box opens (Figure 114).

Figure 114 Rmon History statistics



	14:56:33	14:57:03	14:57:33	14:58:03	14:58:33	14:59:03	14:59:33	15:00:03
SampleIndex	8,297	8,298	8,299	8,300	8,301	8,302	8,303	8,304
Utilization	0	0	0	0	0	0	0	0
Octets	0	0	0	0	0	0	0	0
Pkts	0	0	0	0	0	0	0	0
BroadcastPkts	0	0	0	0	0	0	0	0
MulticastPkts	0	0	0	0	0	0	0	0
DropEvents	0	0	0	0	0	0	0	0
CRCAlignErrors	0	0	0	0	0	0	0	0
UndersizePkts	0	0	0	0	0	0	0	0
OversizePkts	0	0	0	0	0	0	0	0
Fragments	0	0	0	0	0	0	0	0
Collisions	0	0	0	0	0	0	0	0

Table 86 describes the Rmon History statistics tab fields.

Table 86 Rmon History statistics tab fields

Field	Description
SampleIndex	Indicates the sample number. As history samples are taken, they are assigned greater sample numbers
Utilization	Estimates the percentage of a link's capacity that was used during the sampling interval.
Octets	The number of octets received on the link during the sampling period.
Pkts	The number of packets received on the link during the sampling period.
BroadcastPkts	The number of packets received on the link during the sampling interval that destined for the packet address.
MulticastPkts	The number of packets received on the link during the sampling interval that are destined for the multicast address. This doe not include the broadcast packets.
DropEvents	The number of received packets that were dropped due to system resource constraints.

Table 86 Rmon History statistics tab fields (continued)

Field	Description
CRCAlignErrors	The number of packets received during a sampling interval that were between 64 and 1518 octets long. This length included Frame Check Sequence (FCS) octets but not framing bits. The packets had a bad FCS with either an integral number of octets (FCS Error), or a non-integral number of octets (Alignment Error).
UndersizePkts	The number of packets received during the sampling interval were less than 64 octets long (including FCS octets, but not framing bits.
OversizePkts	The number of packets received during the sampling interval were longer than 1518 octets (including FCS octets, but not framing bits, and were otherwise well formed.
Fragments	The number of packets received during the sampling interval were less than 64 octets long (including FCS octets, but not framing bits. The packets had a bad FCS with either an integral number of octects (FCS Error), or a non-integral number of octets (Alignment Error).
Collisions	The best estimate of the number of collisions on an Ethernet segment during a sampling interval.

Enabling Ethernet statistics gathering

You can use RMON to gather Ethernet statistics.

To gather Ethernet statistics:

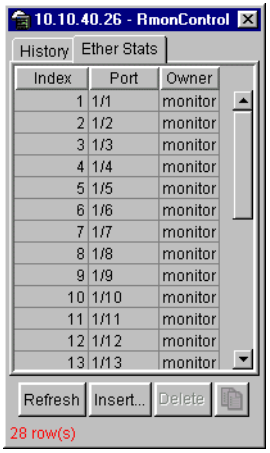
1 From the Device Manager main menu, choose RMON > Control.

The RMONControl dialog box opens with the History tab displayed.

2 Click the Ether Stats tab.

The Ether Stats tab opens (Figure 115).

Figure 115 RMONControl dialog box — Ether Stats tab



3 Click Insert.

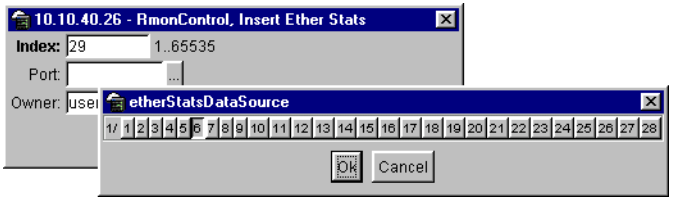
The RMONControl, Insert Ether Stats dialog box opens (Figure 116).

Figure 116 RMONControl, Insert Ether Stats dialog box

4 Select the port(s).

Enter the port number you want or select the port from the list menu (Figure 117).

Figure 117 RMONControl, Insert Ether Stats dialog box port list


10.10.40.26 - RmonControl, Insert Ether Stats
Index: 29
1..65535
Port:
Owner:
etherStatsDataSource
1/ 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28
Ok
Cancel

Device Manager assigns the index.

5 Click Insert.

The new Ethernet Statistics entry is shown in the Ether Stats tab.

Table 87 describes the Ether Stats tab fields.

Table 87 Ether Stats tab fields

Field	Description
Index	A unique value assigned to each interface. An index identifies an entry in a table.
Port	Any Ethernet interface on the device.
Owner	The network management system which created this entry.

Disabling Ethernet statistics gathering

To disable Ethernet statistics that you have set:

1 From the Device Manager main menu, choose RMON > Control.

The RMONControl dialog box opens with the History tab displayed.

2 Click the Ether Stats tab.

The Ether Stats tab opens (Figure 115).

3 Highlight the row that contains the port ID you want to delete.

4 Click Delete.

The Ether Stats entry is removed from the table.

Alarms

Alarms are useful when you need to know when the values of a variable go out of range. You can define an RMON alarm for any MIB variable that resolves to an integer value. You cannot use string variables (such as system description) as alarm variables.

All alarms share the following characteristics:

- An upper and lower threshold value is defined.
- A corresponding rising and falling event occurs.
- An alarm interval or polling period is reached.

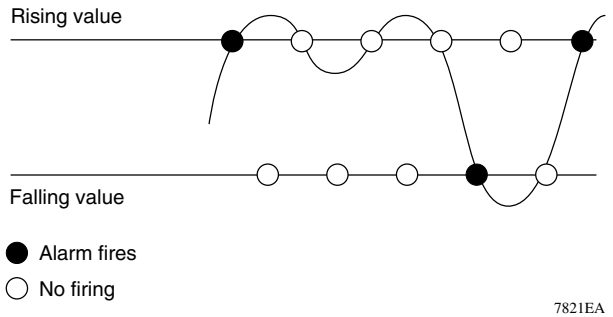
When alarms are activated, you can view the activity in a log or a trap log, or you can create a script to notify you by beeping a console, sending e-mail, or calling a pager.

How RMON alarms work

The alarm variable is polled and the result is compared against upper and lower limit values you select when you create the alarm. If either limit is reached or crossed during the polling period, then the alarm fires and generates an event that you can view in the event log or the trap log.

The alarm's upper limit is called the *rising value*, and its lower limit is called the *falling value*. RMON periodically samples the data based upon the alarm interval. During the *first* interval that the data passes above the rising value, the alarm fires as a rising event. During the first interval that the data drops below the falling value, the alarm fires as a falling event (Figure 118).

Figure 118 How alarms fire



It is important to note that the alarm fires during the first interval that the sample goes out of range. No additional events are generated for that threshold until the opposite threshold is crossed. Therefore, it is important to carefully define the rising and falling threshold values for alarms to work as expected. Otherwise, incorrect thresholds causes an alarm to fire at every alarm interval.

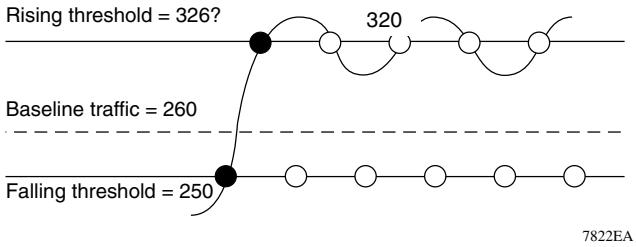
A general guideline is to define one of the threshold values to an expected, baseline value, and then define the opposite threshold as the out-of-bounds limit. Because of sample averaging, the value may be equal to ±1 of the baseline units. For example, assume an alarm is defined on octets going out of a port as the variable. The intent of the alarm is to provide notification to the system administrator when excessive traffic occurs on that port. If spanning tree is enabled, then 52 octets are transmitted out of the port every 2 seconds, which is equivalent to baseline traffic of 260 octets every 10 seconds. This alarm should provide the notification the system administrator needs if the lower limit of octets going out is defined at 260 and the upper limit is defined at 320 (or at any value greater than 260 + 52 = 312).

The first time outbound traffic other than spanning tree Bridge Protocol Data Units (BPDUs) occurs, the rising alarm fires. When outbound traffic other than spanning tree ceases, the falling alarm fires. This process provides the system administrator with time intervals of any nonbaseline outbound traffic.

If the alarm is defined with a falling threshold less than 260 (assuming the alarm polling interval is 10 seconds), say 250, then the rising alarm can fire only once (Figure 119). The reason is that for the rising alarm to fire a second time, the falling alarm (the opposite threshold) must fire. Unless the port becomes inactive

or spanning tree is disabled (which would cause the value for outbound octets to drop to zero), the falling alarm cannot fire because the baseline traffic is always greater than the value of the falling threshold. By definition, the failure of the falling alarm to fire prevents the rising alarm from firing a second time.

Figure 119 Alarm example — threshold less than 260



Creating alarms

When you create an alarm, you select a variable from the variable list and a port, or other switch component, to which it is connected. Some variables require port IDs, card IDs, or other indices (for example, spanning tree group IDs). You then select a rising and a falling threshold value. The rising and falling values are compared against the actual value of the variable that you choose. If the variable falls outside of the rising or falling value range, an alarm is triggered and an event is logged or trapped.

When you create an alarm, you also select a sample type, which can be either absolute or delta. *Absolute* alarms are defined on the cumulative value of the alarm variable. An example of an alarm defined with absolute value is card operating status. Because this value is not cumulative, but instead represents states, such as card up (value 1) and card down (value 2), you set it for absolute value. Therefore, an alarm could be created with a rising value of 2 and a falling value of 1 to alert a user to whether the card is up or down.

Most alarm variables related to Ethernet traffic are set to *delta* value. Delta alarms are defined based on the difference in the value of the alarm variable between the start of the polling period and the end of the polling period. Delta alarms are sampled twice per polling period. For each sample, the last two values are added together and compared to the threshold values. This process increases precision

and allows for the detection of threshold crossings that span the sampling boundary. If you track the current values of a given delta-valued alarm and add them together, therefore, the result is twice the actual value. (This result is not an error in the software.)

Alarm Manager example

Note: The example alarm described in the following procedure generates at least one alarm every five minutes. The example is intended only to demonstrate how alarms fire; it is not a useful alarm. Because of the high frequency, you may want to delete this alarm and replace it with a practical setting.

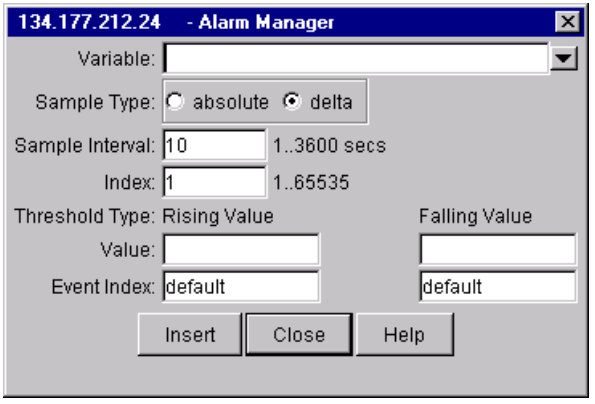
To create an alarm to receive statistics and history using default values:

1 Do one of the following:

- From the Device Manager main menu, choose RMON >Alarm Manager.
- On the toolbar, click the Alarm Manager button.

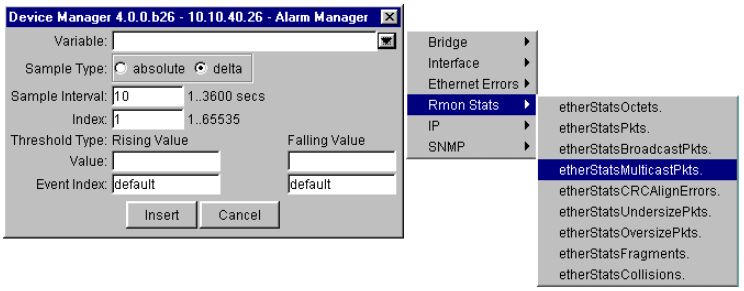
The Alarm Manager dialog box opens (Figure 120).

Figure 120 Alarm Manager dialog box



2 In the variable field, select a variable for the alarm from the list and a port (or other ID) on which you want to set an alarm (Figure 121).

Figure 121 Alarm variable list



Alarm variables are in three formats, depending on the type:

- A chassis alarm ends in .x where the x index is hard-coded. No further information is required.
- A card, spanning tree group (STG) or EtherStat alarm ends with a dot (.). You must enter a card number, STG ID, IP address, or EtherStat information.
- A port alarm ends with no dot or index and requires using the port shortcut menu. An example of a port alarm would be ifInOctets (interface incoming octet count).

  For this example, select Bridge > dot1dStpTopChanges.0 from the variable list. This example is a chassis alarm, indicated by the ".0" in the variable.

3 For this example, select a rising value of 4 and a falling value of 0.

4 Leave the remaining fields at their default values, including a sample type of Delta.

5 Click Insert.

If you want to make field changes, see the field descriptions shown in Table 88.

Table 88 RMON Insert Alarm dialog box fields

Field	Description	
Variable	Name and type of alarm—indicated by the format: *alarmname.x* where x=0 indicates a chassis alarm. *alarmname.* where the user must specify the index. This will be a card number for module-related alarms, an STG ID for spanning tree group alarms (the default STG is 1, other STG IDs are user-configured), or the Ether Statistics Control Index for RMON Stats alarms *alarmname* with no dot or index is a port-related alarm and results in display of the port selection tool.	
Sample Type	Can be either absolute or delta. For more information about sample types, refer to "Creating alarms" on page 221.	
Sample Interval	Time period (in seconds) over which the data is sampled and compared with the rising and falling thresholds.	
Index	Uniquely identifies an entry in the alarm table. Each such entry defines a diagnostic sample at a particular interval for an object on the device.	
Threshold Type	Rising Value	Falling Value
Value	When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, generates a single event.	When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, generates a single event.
Event Index	Index of the event entry that is used when a rising threshold is crossed. The event entry identified by a particular value of this index is the same as identified by the same value of the event index object. (Generally, accept the default that is already filled in.)	Index of the event entry that is used when a falling threshold is crossed. The event entry identified by a particular value of this index is the same as identified by the same value of the event index object. (Generally, accept the default that is already filled in.)

To view the RMON statistics and history for the port for which you have created an alarm:

1 Select the port on which you have created an alarm.

2 From the Device Manager main menu, choose RMON > Control.

The RMONControl dialog box opens displaying the History tab (Figure 112).

3 Click the Ether Stats tab to view statistics (Figure 110 on page 210).

The RMONAlarms dialog box opens with the Alarms tab (Figure 122) displayed.

To delete an alarm:

1 From the Device Manager main menu, choose RMON >Alarms.

The RMONAlarms dialog box opens with the Alarms tab (Figure 122) displayed.

Figure 122 RMONAlarms dialog box — Alarms tab

2 Click any field for the alarm that you want to delete to highlight it.

3 Click Delete.

Table 89 describes the fields on the Alarms tab.

Table 89 Alarms tab fields

Field	Description
Index	Uniquely identifies an entry in the alarm table. Each such entry defines a diagnostic sample at a particular interval for an object on the device
Interval	The interval in seconds over which data is sampled and compared with the rising and falling thresholds. When setting this variable, note that in the case of deltaValue sampling, you should set the interval short enough so that the sampled variable is very unlikely to increase or decrease by more than 2^31 - 1 during a single sampling interval.
Variable	The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of INTEGER (INTEGER, Counter, Gauge, or TimeTicks) may be sampled.

Table 89 Alarms tab fields (continued)

Field	Description
Sample Type	The method of sampling the selected variable and calculating the value to be compared against the thresholds. If the value of this object is absoluteValue(1), the value of the selected variable will be compared directly with the thresholds at the end of the sampling interval. If the value of this object is deltaValue(2), the value of the selected variable at the last sample will be subtracted from the current value, and the difference compared with the thresholds.
Value	The value of the statistic during the last sampling period. For example, if the sample type is deltaValue, this value is the difference between the samples at the beginning and end of the period. If the sample type is absoluteValue, this value is the sampled value at the end of the period. This is the value that is compared with the rising and falling thresholds. The value during the current sampling period is not made available until the period is completed and remains available until the next period completes.
StartupAlarm	The alarm that may be sent when this entry is first set to valid. If the first sample after this entry becomes valid is greater than or equal to the risingThreshold and alarmStartupAlarm is equal to risingAlarm(1) or risingOrFallingAlarm(3), then a single rising alarm is generated. If the first sample after this entry becomes valid is less than or equal to the fallingThreshold and alarmStartupAlarm is equal to fallingAlarm(2) or risingOrFallingAlarm(3), then a single falling alarm is generated.
RisingThreshold	A threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event is generated. A single event is also generated if the first sample after this entry becomes valid is greater than or equal to this threshold and the associated alarmStartupAlarm is equal to risingAlarm(1) or risingOrFallingAlarm(3). After a rising event is generated, another such event is not generated until the sampled value falls below this threshold and reaches the alarmFallingThreshold.
RisingEventIndex	The index of the eventEntry that is used when a rising threshold is crossed. The eventEntry identified by a particular value of this index is the same as identified by the same value of the eventIndex object. If there is no corresponding entry in the eventTable, then no association exists. In particular, if this value is zero, no associated event is generated, because zero is not a valid event index.
FallingThreshold	A threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single event is generated. A single event is also generated if the first sample after this entry becomes valid is less than or equal to this threshold and the associated alarmStartupAlarm is equal to fallingAlarm(2) or risingOrFallingAlarm(3). After a falling event is generated, another such event is not generated until the sampled value rises above this threshold and reaches the alarmRisingThreshold.
FallingEventIndex	The index of the eventEntry that is used when a falling threshold is crossed. The eventEntry identified by a particular value of this index is the same as identified by the same value of the eventIndex object. If there is no corresponding entry in the eventTable, then no association exists. In particular, if this value is zero, no associated event is generated, because zero is not a valid event index.

Table 89 Alarms tab fields (continued)

Field	Description
Owner	The network management system which created this entry.
Status	The status of this alarm entry.

Events

RMON events and alarms work together to notify you when values in your network are outside of a specified range. When values pass the specified ranges, the alarm is triggered and "fires." The event specifies how the activity is recorded.

How events work

An event specifies whether a trap, a log, or a trap and a log is generated to view alarm activity. When RMON is globally enabled, two default events are generated:

- RisingEvent
- FallingEvent

The default events specify that when an alarm goes out of range, the "firing" of the alarm will be tracked in both a trap and a log. For example, when an alarm fires at the rising threshold, the rising event specifies that this information be sent to both a trap and a log. Likewise, when an alarm passes the falling threshold, the falling event specifies that this information be sent to a trap and a log.

Viewing an event

To view a table of events:

1 From the Device Manager main menu, choose RMON > Alarms.

The RMONAlarms dialog box opens displaying the Alarms tab (Figure 122 on page 225).

2 Click the Events tab.

The Events tab opens (Figure 123).

Figure 123 RMONAlarms dialog box — Events tab

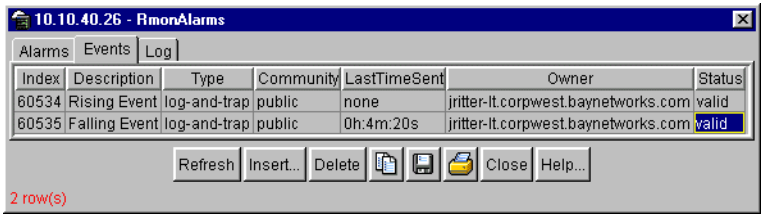


Table 90 describes the RMONAlarms Events tab fields.

Table 90 Events tab fields

Field	Description
Index	This index uniquely identifies an entry in the event table. Each entry defines one event that is to be generated when the appropriate conditions occur.
Description	Specifies whether the event is a rising or falling event.
Type	The type of notification that the Device Manager provides about this event. In the case of log, an entry is made in the log table for each event. In the case of trap, an SNMP trap is sent to one or more management stations. Possible notifications follow: • none • log • trap • log-and-trap
Community	The SNMP community string acts as a password. Only those management applications with this community string can view the alarms.
LastTimeSent	The value of sysUpTime at the time this event entry last generated an event. If this entry has not generated any events, this value is zero.
Owner	If traps are specified to be sent to the owner, then this is the name of the machine that will receive alarm traps.
Status	Normally valid. A not-valid field indicates that an SNMP agent other than the Device Manager has tried to modify an RMON parameter or that network conditions have corrupted an SNMP packet sent by the Device Manager. The status would temporarily appear as “under creation” and then the status would become either “valid” or the field would be deleted.

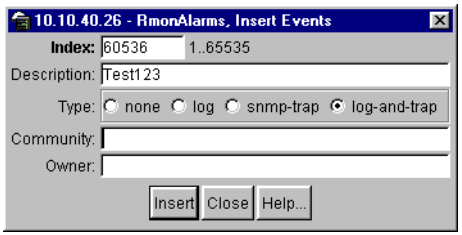
Creating an event

To create an event:

1 In the RMONAlarms dialog box Events tab, click Insert.

The RMONAlarms, Insert Events dialog box opens (Figure 124).

Figure 124 Insert Events dialog box



2 In the Description field, type a name for the event.

3 Select the type of event you want.

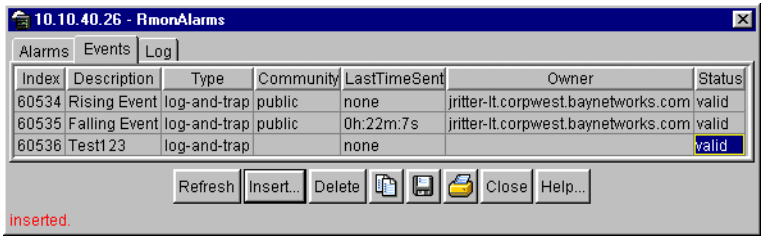
The default setting is log-and-trap. You can set the event type to log to save memory or to snmp-trap to reduce traffic from the switch or for better CPU utilization.

If you select snmp-trap or log-and-trap, you must set trap receivers.

4 Click Insert.

The new event is shown in the Events tab (Figure 125).

Figure 125 New event in the Events tab



Deleting an event

To delete an event:

1 In the Events tab, highlight an event Description.

2 Click Delete.

The event is removed from the table.

Log information

The Log tab chronicles and describes the alarm activity, which is then generated to viewed.

To view the Log tab:

1 From the Device Manager main menu, choose RMON > Alarms.

The RMONAlarm dialog box opens with the Alarms tab displayed (Figure 122 on page 225).

2 Click the Log tab.

The Log tab opens (Figure 126).

Figure 126 Log tab

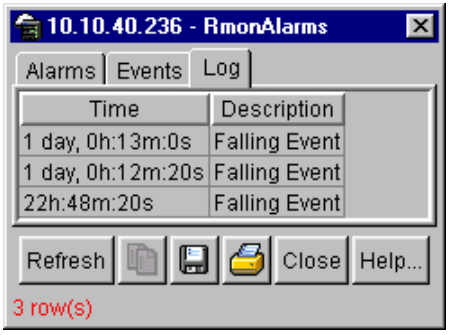


Table 91 describes the Log tab fields.

Table 91 Log tab fields

Item	Description
Time	An implementation-dependent description of the event that activated the log entry.
Description	Specifies whether the event is a rising or falling event.

HP OpenView

You can integrate RMON into HP OpenView. To do so, you must set the HP OpenView path to include the UNIX environment variable. The path is set in the .cshrc file.

To see the path;

1 Enter:

```
setenv | grep PATH
```

A path is displayed similar to this:

```
PATH=/usr/local/

xemacs/bin/sparc-sun-solaris2.4:

bin:/sbin:/usr/sbin:/usr/ccs/bin:/usr/dt/bin:/usr/
openwin/bin:/

usr/etc:/usr/ucb:/usr/local/bin:/usr/local/share/lib:/
usr/
local/

share/bin:/opt/OV/bin:/home/jblogs/bin:.
```

2 Ensure that the HP OpenView directory is in path /opt/OV/bin.

MIB files are shipped with the Device Manager and are located in the following directory:

```
dm/hpov/baystack_mibs
```

3 Load each of the MIB files in the following order:

- bayAgent.mib
- bayChas.mib
- bayChasTraps.mib
- bayEMTmib
- baylfex.mib
- bayS5Reg.mib
- bayS5Rt.mib
- bayS5Tcs.mib
- baySRoot.mib
- rc_vlan.mib
- rfc1213.mib
- rfc1215.mib
- rfc1447.mib
- rfc1450.mib
- rfc1493.mib
- rfc1573_bs.mib
- rfc1573_rcc.mib
- rfc1643.mib
- rfc1757.mib
- rfc1757_rcc.mib
- rfc1907.mib

Now you can start HP OpenView.

Log only event bug

HP OpenView versions 4.0 and 5.0 contain bugs that do not affect the integrity of the product when it stands alone. However, when combined with Device Manager, unexpected results occur.

The “Log only” event categorization bug in HP OpenView 4.0 causes traps to be written to the ASCII trap log file and to be displayed in the event browser.

The default category for SNMP traps, such as “link up” and “link down,” happens to be “Log only.” The correct procedure for an event (trap) with a “Log only” categorization is that it should only be written to the ASCII trap log file.

In version 4.0, standard SNMP traps are displayed in the event browser when the default category of “Log only” is selected. However, SNMP traps are not displayed in the event browser version 5.0, because this bug is fixed. If you were not aware that version 4.0 had a problem, then you may have erroneously assumed that the switch was not sending these traps. In this case, you can view the ASCII trap log file. Enter:

```
/var/opt/OV/share/log/trapd.log
```

When you view the log, you can verify that the switch is sending the traps. In fact, when both HP OpenView and Device Manager are running on a machine, and that machine is configured on the switch as a trap receiver, HP OpenView receives the trap. HP OpenView then passes the trap to Device Manager. If Device Manager displays a trap, HP OpenView has also received the trap.

To have standard SNMP traps displayed in the event browser for HP OpenView 5.0:

1. From the Options menu, choose Event Configuration.
2. Select enterprise name snmpTraps.
3. Double-click the event (trap) name you want.
4. Change the category from Log Only to any event type.

   Your choices are Error Events, Threshold Events (normally used for RMON alarms), Status Events, Configuration Events, or Application Alert Events.

5 Click OK.

6 Choose File > Save.

Chapter 11
Security parameters

You can set the security features for a switch so that the actions are performed by the software when a violation occurs. The security actions you specify are applied to all ports of the switch.

This chapter describes the Security information available in Device Manager on the following tabs:

- General tab (next)
- AuthConfig tab (page 240)
- SecurityList tab (page 243)
- AuthStatus tab (page 243)
- AuthViolation (page 245)

General tab

The General tab allows you to set and view general security information for the switch.

To view the General tab:

➨ From the Device Manager menu bar, select Edit > Security.

The Security dialog box opens with the General tab displayed (Figure 127).

Figure 127 General tab

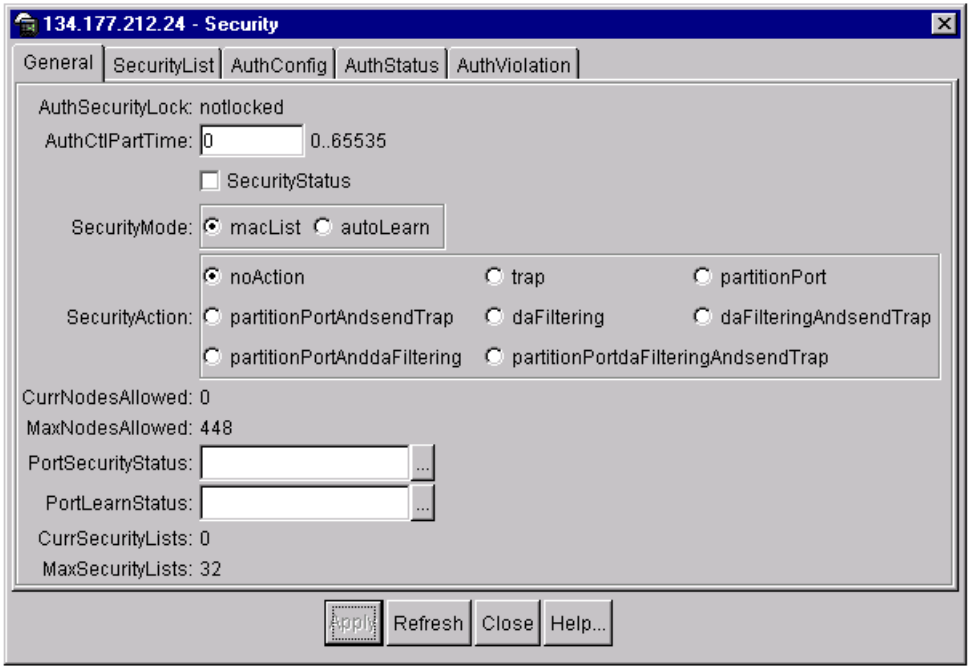


Table 92 describes the General tab items.

Table 92 General tab items

Items	Description
AuthSecurityLock	If this parameter is listed as “locked,” the agent refuses all requests to modify the security configuration. Entries also include: • other • notlocked
AuthCtlPartTime	This value indicates the duration of the time for port partitioning in seconds. Default: 0 (zero). When the value is zero, port remains partitioned until it is manually re-enabled.
SecurityStatus	Indicates whether or not the switch security feature is enabled.
SecurityMode	Mode of switch security. Entries include: • macList: Indicates that the switch is in the MAC-list mode. You can configure more than one MAC address per port. • autoLearn: Indicates that the switch learns the first MAC address on each port as an allowed address of that port.

Table 92 General tab items (continued)

Items	Description
SecurityAction	Actions performed by the software when a violation occurs (when SecurityStatus is enabled). The security action specified here applies to all ports of the switch. A blocked address causes the port to be partitioned when unauthorized access is attempted. Selections include: • noAction: Port does not have any security assigned to it, or the security feature is turned off. • trap: Listed trap. • partitionPort: Port is partitioned. • partitionPortAndsendTrap: Port is partitioned and traps are sent to the trap receive station. • daFiltering: Port filters out the frames where the destination address field is the MAC address of unauthorized Station. • daFilteringAndsendTrap: Port filters out the frames where the desitnation address field is the MAC address of unauthorized station. Traps are sent to trap receive station(s). • partitionPortAnddaFiltering: Port is partitioned and will filter out the frames with the destination address field is the MAC address of unauthorized station. • partitionPortdaFilteringAndsendTrap: Port is partitioned and will filter out the frames with the destination address field is the MAC address of unauthorized station. Traps are sent to trap receive station(s). **Note**: “da” means destination address.
CurrNodesAllowed	Current number of entries of the nodes allowed in the AuthConfig tab.
MaxNodesAllowed	Maximum number of entries of the nodes allowed in the AuthConfig tab.
PortSecurityStatus	Set of ports for which security is enabled.
PortLearnStatus	Set of ports where auto-learning is enabled.
CurrSecurityLists	Current number of entries of the Security listed in the SecurityList tab
MaxSecurityLists	Maximum entries of the Security listed in the SecurityList tab.

SecurityList tab

The SecurityList tab contains a list of Security port items.

To view the SecurityList tab:

1 From the Device Manager menu bar, select Edit > Security.

The Security window opens with the General tab displayed (Figure 127).

2 Click the SecurityList tab.

The SecurityList tab opens (Figure 128).

Figure 128 SecurityList tab

Table 93 describes the SecurityList tab fields.

Table 93 SecurityList tab fields

Field	Description
SecurityListIndx	An index of the security list. This corresponds to the Security port list that can be used as an index into AuthConfig tab.
SecurityListMembers	The set of ports that are currently members in the Port list.

Security, Insert SecurityList dialog box

Security, Insert SecurityList dialog box has editable fields for the SecurityList tab. Each row in this dialog box has information that can be updated or changed.

To view the Security, Insert AuthConfig dialog box:

1 From the Device Manager menu bar, select Edit > Security.

The Security window opens with the General tab displayed.

2 Click the SecurityList tab.

The SecurityList tab opens (Figure 128).

3 Click inside a row.

4 Click Insert.

The Security, Insert SecurityList dialog box opens (Figure 129).

Figure 129 Security, Insert SecurityList dialog box

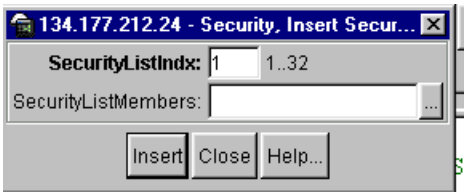


Table 94 describes the Security, Insert AuthConfig dialog box items.

Table 94 Security, Insert AuthConfig dialog box fields

Field	Description
SecurityListIndx	An index of the security list. This corresponds to the Security port list that can be used as an index into AuthConfig tab.
SecurityListMembers	The set of ports that are currently members in the Port list.

AuthConfig tab

The AuthConfig tab contains a list of boards, ports and MAC addresses that have the security configuration. An SNMP SET PDU for a row in the tab requires the entire sequence of the MIB objects in each entry to be stored in one PDU. Otherwise, GENERR return-value is returned.

To view the AuthConfig tab:

1 From the Device Manager menu bar, select Edit > Security.

The Security window opens with the General tab displayed (Figure 127).

2 Click the AuthConfig tab.

The AuthConfig tab opens (Figure 130).

Figure 130 AuthConfig tab

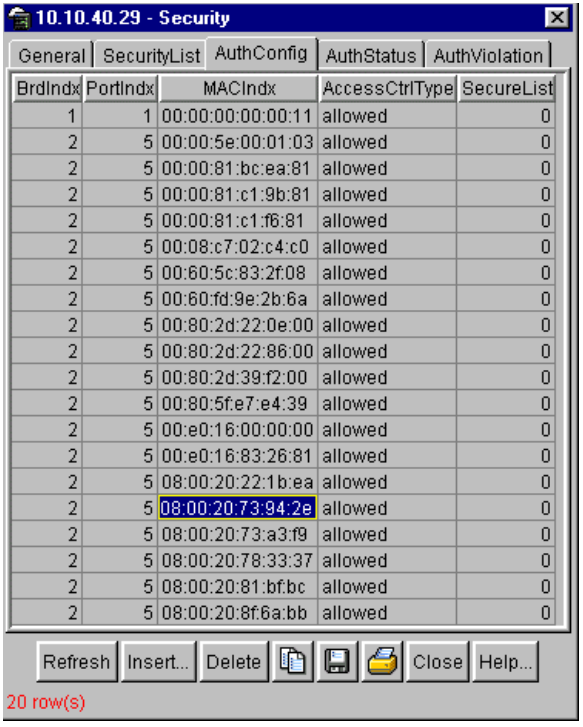


Table 95 describes the AuthConfig tab fields.

Table 95 AuthConfig tab fields

Field	Description
BrdIndx	Index of the slot containing the board on where the port is located. This value is meaningful only if SecureList value is zero. For other SecureList values, this parameter should have the value of zero.
PortIndx	Index of the port on the board. This value is meaningful only if SecureList value is zero. For other SecureList values, this parameter should have the value of zero.
MACIndx	An index of MAC addresses that are either designated as `allowed` (station) or `not-allowed` (station).
AccessCtrlType	Displays whether the node entry is `node allowed` or `node blocked`. A MAC address may be allowed on multiple ports.
SecureList	The index of the security list. This value is meaningful only if BrdIndx and PortIndx values are set to zero. For other board and port index values, it should also have the value of zero. The corresponding MAC Address of this entry is allowed or blocked on all ports of that this port list.

Security, Insert AuthConfig dialog box

Security, Insert AuthConfig dialog box has editable fields for the AuthConfig tab. Each row in this dialog box has information that can be updated or changed.

To view the Security, Insert AuthConfig dialog box:

1. From the Device Manager menu bar, select Edit > Security.

   The Security window opens with the General tab displayed.

2. Click the AuthConfig tab.

   The AuthConfig tab opens (Figure 130).

3. Click inside a row.
4. Click Insert.

   The Security, Insert AuthConfig dialog box opens (Figure 131).

Figure 131 Security, Insert AuthConfig dialog box

Table 96 describes the Security, Insert AuthConfig dialog box fields.

Table 96 Security, Insert AuthConfig dialog box fields

Item	Description
BrdIndx	Index of the board. This corresponds to the index of the slot containing the board, but only if the index is greater than zero. A zero index is a wild card.
PortIndx	Index of the port on the board. This corresponds to the index of the last manageable port on the board, but only if the index is greater than zero. A zero index is a wild card.
MACIndx	An index of MAC addresses that are either designated as `allowed` (station) or `not-allowed` (station).
AccessCtrlType	Displays whether the node entry is `node allowed` or `node blocked`. A MAC address may be allowed on multiple ports.
SecureList	The index of the security list. This value is meaningful only if BrdIndx and PortIndx values are set to zero. For other board and port index values, it should also have the value of zero. The corresponding MAC Address of this entry is allowed or blocked on all ports of that this port list.

AuthStatus tab

The AuthStatus tab displays information of the authorized boards and port status data collection. Information includes actions to be performed when an unauthorized station is detected and the current security status of a port. An entries in this tab may include:

- A single MAC address
- All MAC addresses on a single port
- A single port
- All the ports on a single board
- A particular port on all the boards
- All the ports on all the boards.

To view the AuthStatus tab:

1. From the Device Manager menu bar, select Edit > Security.

   The Security window opens with the General tab displayed (Figure 127).

2. Click the AuthStatus tab.

   The AuthStatus tab opens (Figure 132).

Figure 132 AuthStatus tab

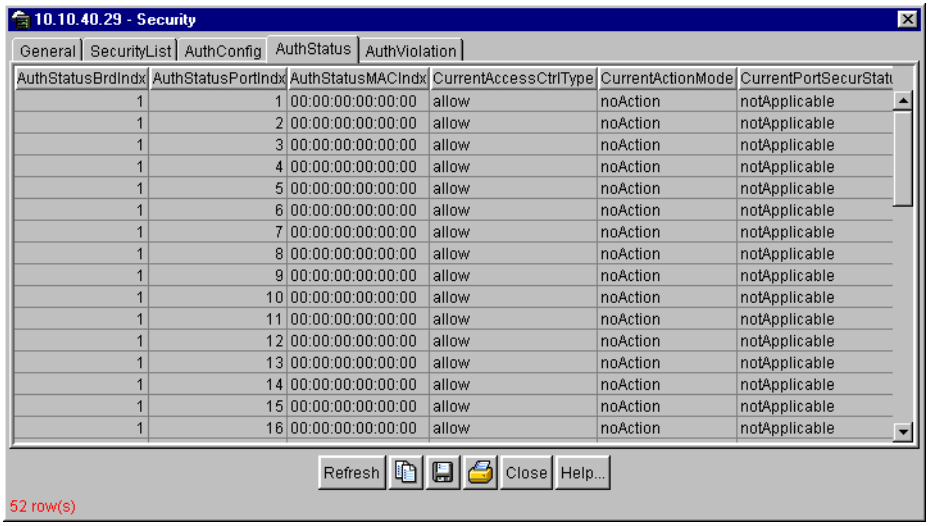


Table 97 describes the AuthStatus tab fields.

Table 97 AuthStatus tab fields

Item	Description
AuthStatusBrdIndx	The index of the board. This corresponds to the index of the slot containing the board if the index is greater than zero.
AuthStatusPortIndx	The index of the port on the board. This corresponds to the index of the last manageable port on the board if the index is greater than zero.
AuthStatusMACIndx	The index of MAC address on the port. This corresponds to the index of the MAC address on the port if the index is greater than zero.
CurrentAccessCtrlType	Displays whether the node entry is `node allowed` or `node blocked type`.

Table 97 AuthStatus tab fields (continued)

Item	Description
CurrentActionMode	A value representing the type of information contained, including: noAction: Port does not have any security assigned to it, or the security feature is turned off. partitionPort: Port is partitioned. partitionPortAndsendTrap: Port is partitioned and traps are sent to the trap receive station. Filtering: Port filters out the frames, where the destination address field is the MAC address of unauthorized station. FilteringAndsendTrap: Port filters out the frames, where the destination address field is the MAC address of unauthorized station. Trap are sent to trap receive station. sendTrap: A trap is sent to trap receive station(s). partitionPortAnddaFiltering: Port is partitioned and will filter out the frames with the destination address field is the MAC address of unauthorized station. partitionPortdaFilteringAndsendTrap: Port is partitioned and will filter out the frames with the destination address field is the MAC address of unauthorized station. Traps are sent to trap receive station(s).
CurrentPortSecurStatus	Displays the security status of the current port, including: • If the port is disabled, notApplicable is returned. • If the port is in a normal state, portSecure is returned. • If the port is partitioned, portPartition is returned.

AuthViolation tab

The AuthViolation tab contains a list of boards and ports where network access violations have occurred, and also the identity of the offending MAC addresses.

To view the AuthViolation tab:

1 From the Device Manager menu bar, select Edit > Security.

The Security window opens with the General tab displayed (Figure 127).

2 Click the AuthViolation tab.

The AuthViolation tab opens (Figure 133).

Figure 133 AuthViolation tab

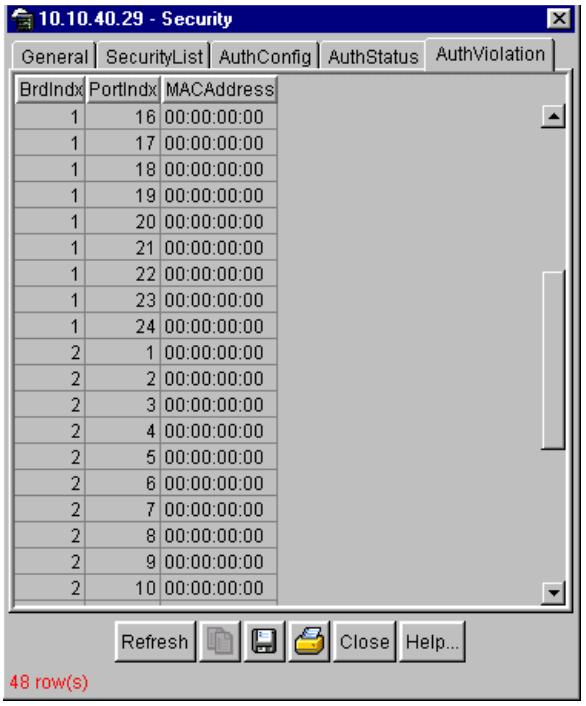


Table 98 describes fields for the AuthViolation tab fields.

Table 98 AuthViolation tab fields

Field	Description
BrdIndx	The index of the board. This corresponds to the slot containing the board. The index will be 1 where it is not applicable.
PortIndx	The index of the port on the board. This corresponds to the port on that a security violation was seen.
MACAddress	The MAC address of the device attempting unauthorized network access (MAC address-based security).

Index

Numbers

1..64 field 112
1024..1518 field 112
128..255 field 112
256..511 field 112
511..1023 field 112
65..127 field 112

A

AbsoluteValue statistics 44
access levels 31
Action field 74
Actions menu 34
ActiveMember field 129
ActiveMembers field 139
ActiveQuerier field 138
Addr field 55
AddrMaskReps field 82, 84
AddrMasks field 82, 84
Admin field 61
AdminControlledDirections field 95, 101
AdminDuplex field 89, 98
AdminSpeed field 89, 98
AdminState field 63
AdminStatus field 88, 98
Agent Info tab 65
Alarm Manager button 35
alarms tab 225
alarms, RMON
  characteristics of 219
  creating 221
AlignmentErrors field 107, 125
allocating bandwidth 34
Area Chart button 50
area graph example 45
ARP tab 56
AuthConfig tab
  AccessCtrlType field 241
  BrdIndx field 241
  MACIndx field 241
  PortIndx field 241
  SecureList field 241
AuthControlledPortControl field 95, 101
AuthControlledPortStatus field 95, 101
AuthEapLogoffWhileAuthenticated field 117
AuthEapLogoffWhileAuthenticating field 116
AuthEapStartsWhileAuthenticated field 117
AuthEapStartsWhileAuthenticating field 116
AuthenticationTraps field 59
AuthFailWhileAuthenticating field 116
AuthReauthsWhileAuthenticated field 116
AuthReauthsWhileAuthenticating field 116
AuthStatus tab
  AuthStatusBrdIndx field 244
  AuthStatusMACIndx field 244
  AuthStatusPortIndx field 244
  CurrentAccessCtrlType field 244
  CurrentActionMode field 245
  CurrentPortSecurStatus field 245
AuthSuccessWhileAuthenticating field 116

AuthTimeoutsWhile Authenticating field 116
AuthViolation tab
BrdIndx field 246
MACIndx field 246
PortIndx field 246
AutoNegotiate field 89, 98
Average statistics 44

B

BackendAccessChallenges field 117
BackendAuthFails field 117
BackendAuthState field 95, 101
BackendAuthSuccesses field 117
BackendNonNakResponsesFromSupplicant field 117
BackendOtherRequestsToSupplicant field 117
BackendResponses field 117
Bar Chart button 50
Base tab 197
BcastAddr field 55
BkplType field 207
blinking LEDs 39
BootMode field 59
BootRouterAddr tab 65
Bridge dialog box 197
Bridge parameter
Base tab
BridgeAddress field 198
NumPorts field 198
Type 198
Forwarding tab
Address field 204
Port field 204
Status field 204
Spanning Tree tab
BridgeHelloTime field 201
BridgeMaxAge field 200
DesignatedRoot field 200
ForwardDelay field 200
HelloTime field 200
MaxAge field 200
Priority field 199
ProtocolSpecification field 199
RootCost field 200
RootPort field 200
TimeSinceTopologogyChange field 201
TimeSinceTopologyChange field 199
TopChanges field 200
Transparent tab
AgingTime field 202
LearnedEntryDiscard field 202
Bridge tab 109
BridgeAddress field 143, 148
BridgeForwardDelay field 144, 145
BridgeHelloTime field 143, 145
BridgeMaxAge field 143, 145
BroadcastPkts field 111
buckets 211
BucketsGranted field 213
BucketsRequested field 213
buttons
dialog boxes 42
toolbar 35

C

CarrierSenseErrors field 107, 125
chassis
configuration, editing 56
graphing 74
Chassis ICMP In statistics window 81
Chassis ICMP Out statistics tab 83
Chassis SNMP tab 76
ChassisType field 207
class of service 34
Collisions field 112
Color field 129, 139
color-coded ports 38, 39

Common Open Policy Services 34
communication parameters, setting for Device Manager 28
Community field 67, 228
community strings
  default 31
  entering 32
ConfigFileName field 73
configuration
  MAC-SA-based VLAN 133
  Multi-Link Trunks 120
  port-based VLAN 128, 129, 137
  ports 205
  protocol-based VLAN 131
  QoS 155
  STG 144
  STGs 143
  uploading and downloading 72
Confirm row deletion field 30
ConstraintType field 129, 139
Control tab 212
conventions
  text 23
COPS retry setting tab 193
Copy button 42
Copy File tab 72
CRAlignErrors field 111
Cumulative statistics 44
CurrentDefaultGateway field 59
CurrentImageVersion field 59
CurrentMgmtProtocol field 59
CurState field 207
customer support 25

D

data, exporting 48
default access community strings 31
Default TTL field 54
DefaultVLANId field 91, 100
DeferredTransmissions field 108, 126
DelayExceededDiscards field 110
Descr field 61, 63, 69, 70, 88, 97
Description field 228
DesignatedBridge field 92, 150
DesignatedCost field 92
DesignatedPort field 92, 150
DesignatedRoot field 92, 148, 150
DestUnreachs field 82, 84
Device Manager
  setting properties 28
Device Manager window 28
Device menu 34
Device Name field 32
device view
  summary 35
device, opening 31
Differentiated Services 34
Disable command 41
disabled port, color 39
DiscardTagged Frames field 90, 100
DiscardUntaggedFrames field 91, 100
downloading configuration 72

E

EapLengthErrorFramesRx field 114
EapLogoffsWhileConnecting field 116
EAPOL 93, 113, 114
EAPOL Diag tab 114
EAPOL Security 60
EAPOL Stats tab 113
EAPOL tab for multiple ports 100
EapolFramesRx field 114
EapolFramesTx Field 114
EapolLogoffFramesRx field 114

EapolReqFramesTx field 114
EapolReqIdFramesTx field 114
EapolRespFramesRx field 114
EapolRespldFramesRx 114
EapolStartFramesRx field 114
EchoReps field 82, 84
Echos field 82, 84
Edit command 41
Edit menu 34
Edit Selected button 35
Enable 138
Enable command 41
Enable field 30
Enable STP field 144
Enable Stp field 92
EnableStp field 150
EntersAuthenticating field 116
EntersConnecting field 116
Ether Stats Control tab 217
Ethernet Errors tab 106
Ethernet statistics, disabling 218
Event Index field 224
events, RMON 227
ExcessiveCollisions field 108, 126
Export Data button 43, 48

F

falling event 227
falling value, RMON alarms 219
FallingEventIndex field 226
FallingThreshold field 226
Fan tab 70, 71
FastStart field 92, 150
FCSErrors field 107, 125
File System window 72
files
  uploading and downloading 72
ForwardDelay field 148
Forwarding tab 202
ForwardTransistions field 92
ForwardTransitions field 150
ForwDatagrams field 80
FragCreates field 80
FragFails field 80
FragOKs field 80
frames, discarding tagged frames on 136
FrameTooLongs field 108, 125

G

Globals tab 54
Globe button 35
graph
  creating 48
  modifying 50
Graph command 41
graph dialog box 49
Graph menu 34
Graph Selected button 35, 49
graph types 44
graphPort, Interface tab 104

H

HCInBroadcastPkt field 123
HCInMulticastPkt field 123
HCInOctets field 122
HCInUcastPkts field 122
HCOutBroadcast field 123
HCOutMulticast field 123
HCOutUcastPkts field 123
HDOutOctets field 122
HelloTime field 148

Help button 35
Help menu 34
Help, Device Manager 52
HoldTime field 148
Horizontal button 50
HP OpenView, using with RMON 231

I

ICMP In tab 82
ICMP Out statistics 83
ICMP Out tab 83
ID field (VLAN) 134
ifInNUcastPkts field 104
ifInOctets field 104
ifInUcastPkts field 104
ifOutNUcastPkts field 104
ifOutOctets field 104
ifOutUcastPkts field 104
image file 72
ImageFileName field 73
ImageLoadMode field 59
InAddrErrors field 79
InASNParseErrs field 77
InBadCommunityNames field 77
InBadCommunityUses field 77
InBadValues field 77
InBadVersions field 77
InBroadcastPkt field 122
InDelivers field 80
Index field 88, 97, 101, 224
InDiscards field 80, 105, 110
InErrors field 105
InFrames field 110
InGenErrs field 78
InGetNexts field 77
InGetRequests field 76
InGetResponses field 77
InHdrErrors field 79
InMulticastPkts field 122
InNoSuchNames field 77
Inpkts field 76
InReadOnlys field 78
InReceives field 79
Insert Alarm dialog box 222
Insert AuthConfig dialog box
  BrdIndx field 242
Insert button 42
Insert Control dialog box 213
Insert Ether Stats dialog box 217
Insert Event dialog box 229
InSetRequests field 77
interface IDs 157
Interface item
  ARP 56
Interface Queue tab 152
interface queues 151
Interface tab 86
Interface tab for a multiple port 96
Interface window 122
InternalMacReceiveErrors field 107, 125
InternalMacTransmitErrors field 107, 125
Interval field 214, 225
InTooBigs field 77
InTotalReqVars field 76
InTotalSetVars field 76
InUnknownProtos field 80, 105
InvalidEapolFramesRx field 114
IP Address tab 55
IP dialog box 53
IP filter tab 166
IP tab 79

IpAddr field 206, 207
IPAddress field 56

J

Jabbers field 112

K

KeyTxEnabled field 95, 102

L

LastChange field 89, 98
LastEapolFrameSource 96
LastEapolFrameSource field 102
LastEapolFrameVersion field 96, 102
LastLoadProtocol field 60
LastTimeSent field 228
LastUnauthenticatedCommunityString field 66
LastUnauthenticatedIpAddress field 66
LastValue statistics 44
LateCollisions field 108, 126
layer 2 filter group tab 171
LEDs 39
LEDs in device view 39
legend, port color 34, 39
Line Chart button 50
link, lacking, color 39
LoadServerAddr field 73
LocalSeg field 207
LocalStorageImageVersion field 59
Location field 62, 63
Log Scale button 50
Log tab 230
logs 230
LstChng field 61, 63

M

MacAddr field 65, 207
MacAddress field 56
MAC-SA-based VLAN 133
Max Traps in Log field 30
MaxAge field 148
Maximum statistics 44
MaxReq field 95, 102
MDA
  shortcut menu 42
  viewing 37
media dependent adapter. *See* MDA
menu bar, Device Manager 34
menus. *See* individual menu names
Minimum statistics 44
MLT
  requirements 119
MltId field 89, 98
MRouterExpiration field 138
MRouterPorts field 138
Mtu field 88, 97
MtuExceededDiscards field 110
MulticastPkts field 111
Multi-Link Trunk window 121
Multi-Link Trunking. *See* MLT
Multi-Link Trunks window 120
multiple objects, selecting 37
MultipleCollisionFrames field 108, 126

N

Name field 120, 129, 138, 139
NetMask field 55
new table entry, creating 42
NextBootDefaultGateway field 59
NextBootLoadProtocol field 60

NextBootMgmtProtocol field 59
NextBootNetMask field 65
NextBootpAddr field 65
NmmCurNum field 206
NmmLstChg field 206
NmmMaxNum field 206
NoSuchObject error message 86, 96
NumPort field 143, 148

O

object types 36
objects
  editing 43
  selecting 36
Octets field 111
online Help 34, 52
Open Device button 31, 35
Open Device dialog box 31, 34
operating port, color 39
OperControlledDirections field 95, 101
OperSpeed field 89, 98
OperState field 61, 64, 69, 70
OperStatus field 89, 98
OutBadValues field 77
OutBroadcast field 122
OutDiscards field 80, 105
OutErrors field 105
OutFrames field 110
OutGenErrs field 77
OutMulticast field 122
OutNoRoutes field 80
OutNoSuchNames field 77
Outpkts field 76
OutRequests field 80
OutTooBigs field 77
OutTraps field 77
OversizePkts field 112
Owner field 214, 218, 227, 228

P

PaeState 95
PaeState field 101
ParmProbs field 82, 84
Paste button 42
PathCost field 92, 150
PhysAddress field 88, 97
Pkts field 111
Poll 108
polling interval 48
Port Capabilities field 95
port color legend 39
Port dialog box 103
port Ethernet Error Statistics tab 105
Port field 207, 218
Port Interface tab 87, 97
port shortcut menu 41
Port Spanning Tree window 91
port-based VLANs 128
PortCapabilities field 101
PortInitialize field 95, 101
PortMembers field 120, 129, 139, 144, 145
PortProtocolVersion field 95, 101
PortReauthenticate field 95, 101
ports
  color-coded 38, 39
  configuring 85, 205
  controlling 85
  disabled 39
  editing 85, 96
  graphing 86, 103
  selecting 37
  viewing 85, 96
PortType field 120

Power Supply tab 69
Print button 42
Priority field 92, 143, 145, 150
product support 25
Properties dialog box 28, 29
  Hotswap Poll Interval field 30
  If Traps, Status Interval
) field 29
  Status Poll Interval field 29
protocol-based VLAN 131
Protocol-based VLAN window 132
ProtocolId field 129, 139
ProtocolSpecification field 143, 148
publications
  hard copy 25
  related 24

Q

QoS
  displaying layer 2 filters 167
  interface group 156
  interface IDs 157
  interface queues 151
  ports 156
  queues
    QoS
      role combinations 157
  role combinations 156
QoS action tab 173
QoS agent configuration tab 186
QoS capabilities tab 189
QoS configuration tab 191
QoS current tab 190
QoS DSCP mapping tab 162
QoS DSCP Q assign tab 161
QoS Interface group tab 153
QoS interface ID tab 157
QoS Interface Queue tab 152
QoS IP filter tab 163
QoS layer 2 filter tab 168
QoS meters tab 176
QoS policies tab 181
QoS policy class tab 187
QoS policy device identification tab 188
QoS policy statistics tab 185
QoS priority assign tab 159
QoS priority mapping tab 160
QoS shapers tab 179
QoS/COPS menu 34
Quality of Service 34
QuerierPort field 138
QueryInterval field 138
QuietPeriod field 95, 102

R

Read Community field 32
Read Community, SNMP 32
Read Community, SNMP field 32
Read-Write-All access 32
ReasmFails field 81
ReasmMaxSize field 55
ReasmOKs field 81
ReasmReqds field 80
ReasmTimeout field 54
ReAuthEnabled field 95, 102
ReAuthPeriod field 95, 102
Reboot field 59
Rebustness field 138
Redirects field 82, 84
Refresh Device Status button 35
Register for Traps field 30
Remote Monitoring. *See* RMON
Reset Changes button 42

Retry Count field 30
rising event 227
rising value, RMON alarms 219
RisingEventIndex field 226
RisingThreshold field 226
RMON
  alarms
    characteristics 219
    creating 221
    deleting 225
    inserting 223
  events
    definition 227
  history
    creating 212
    definition 211
    disabling 214
  statistics 210, 212
  using HP OpenView with 231
RMON EtherStat tab 111, 210
RMON Event tab 228
Rmon menu 34
RootCost field 148
RootPath field 148

S

Sample Interval field 224
Sample Type field 224, 226
security 93
Security parameters
  General tab
    AuthCtlPartTime field 236
    AuthSecurityLock field 236
    CurrNodesAllowed field 237
    CurrSecurityLists field 237
    MaxNodesAllowed field 237
    MaxSecurityLists field 237
    PortLearnStatus field 237
    PortSecurityStatus field 237
    SecurityAction field 237
    SecurityMode field 236
    SecurityStatus field 236
Security, Insert AuthConfig dialog box
  AccessCtrlType field 242
  MACIndx field 242
  PortIndx field 242
  SecureList field 242
SecurityListIndx field 238
SecurityListMembers 238
SegId field 207
SerNum field 61, 64
ServerTimeout 102
ServerTimeout field 95
shortcut menus
  MDA 42
  port 41
  switch unit 40
single object, selecting 36
SingleCollisionFrames field 108, 126
Slot field 207
SNMP Info tab 66
SNMP tab 65
SNMP traps 51
Snoop tab 137
Spanning Tree Groups 144
Spanning Tree tab 198, 199
Spanning Tree window 91
Speed field 98
SQETestErrors field 108, 126
SrcQuenchs field 82, 84
Stack Info tab 62
Stacked button 50
Standalone Unit Info Tab 61
standby port, color 39
StartupAlarm field 226
State field 92, 150
statistics

Ethernet statistics, enabling 216
for a single object 47
for multiple objects 48
graphing 44
ICMP Out 83
MLT 121
RMON 210, 212
single port 47
types 44
statistics dialog box
multiple objects 48
statistics dialog boxes 34
Status field 74, 206, 227, 228
STG 91
StgId field 92, 129, 139
STGs
creating 144
status 147, 148
Stop button 43
support, Nortel Networks 25
SuppTiemout field 102
SuppTimeout field 95
switch stack, selecting 37
switch unit shortcut menu 40
switch, selecting 36
sysContact field 59
sysDescr field 58
sysLocation field 59
sysName field 59
System tab 58
SystemAuthControl field 60
sysUpTime field 58

T

tagged frame, discarding 136
tagged ports
configuring 136
TaggedBdpuVlanId field 144, 145
technical publications 25
technical support 25
Telnet button 35, 51
Telnet session 34, 35, 50
tested port, color 39
text conventions 23
Threshold Type field 224
TimeExcds field 82, 84
Timeout field 30
TimeSinceTopologyChange field 148
TimestampReps field 82, 84
Timestamps field 82, 84
toolbar, Device Manager 35
TopChanges field 148
topology 205
Trace field 30
Transparent Bridging tab 109, 113, 115
Transparent tab 201
trap log 51
Trap Log button 35
Trap Port field 30
Trap Receivers
NetAddr field 67
Trap Receivers tab 67
troubleshooting
locations of Help files 52
receiving traps 51
selecting switches in device view 37
TrpRcvrCurEnt field 66
TrpRcvrMaxEnt field 66
TrpRcvrNext field 66
TxPeriod field 95, 102
Type 129
Type field 56, 61, 88, 90, 97, 100, 228
types of objects 36

U

UndersizePkts field 112
UNIX
  receiving traps 51
unmanageable port, color 39
upgrading
  to version 2.0 72
uploading configuration 72
UserDefined field 139
UserDefinedPid field 129

V

ValidFlag tab 65
Value field 224, 226
value, changed 43
Variable field 224, 225
Ver field 61, 64
Viewing 85
VLAN 89
VLAN Basic tab 128, 143
VLAN dialog box 129, 138, 143, 145, 148, 150
VLAN menu 34
VLAN tab 90, 94
VLAN tab for multiple ports 99
VlanIds field 90, 100
VLANs
  creating 128
  default 128
  limitations 127
  MAC-SA-based 133
  managing 138
  port-based 128
  protocol-based 131

W

Web session 35
window, Device Manager 33
Write Community field 32
Write Community, SNMP 32